НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
Факультет інформатики та обчислювальної техніки
Кафедра обчислювальної техніки

До захисту допущено:

Завідувач кафедри
_____ Сергій СТІРЕНКО

“___”_____2020 р.

Дипломний проект

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Комп’ютерні системи та мережі»

спеціальності 123 «Комп’ютерна інженерія»

на тему: «Програмні засоби навчання системних адміністраторів використанню можливостей технологій Intel® vPro™: Trusted Execution-Technology»

Виконав:
студент IV курсу, групи ІО-61
Гліб БАЛАЦЕНКО _____

Керівник:
Доцент, к.т.н.,
Олександр ДОЛГОЛЕНКО _____

Консультант з нормоконтролю:
Професор, д.т.н.,
Валерій СІМОНЕНКО _____

Рецензент:

_____

Засвідчую, що у цьому дипломному проекті немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2020

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
Факультет інформатики та обчислювальної техніки
Кафедра обчислювальної техніки

Рівень вищої освіти – перший (бакалаврьский)
Спеціальність – 123 «Комп'ютерна інженерія»
Освітньо-професійна програма «Комп'ютерні системи та мережі»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Сергій СТІРЕНКО

«___» _____2020 р.

ЗАВДАННЯ
на дипломний проект студента

Балаценко Гліба Ігоровича

1. Тема проекту «Програмні засоби навчання системних адміністраторів використанню можливостей технологій Intel® vPro™: Trusted Execution-Technology»

керівник проекту Долголенко Олександр Миколайович, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «07» травня 2020 року №1081-с

2. Термін здачі студентом закінченого проекту

3. Вихідні дані до проекту *технічна документація*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які розробляються)

Опис предметної області, дослідження структури Trusted Execution Technology, розробка серверної платформу Moodle, що орієнтована на вивчення можливостей технологій Intel® vPro™, перевірка середовища запуску та встановлення кореня довіри.

5. Перелік графічного матеріалу

Принципова схема, функціональна схема та структурна схема

6. Консультанти проекту, з вказівкою розділів роботи, які до них вносяться

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
нормоконтроль	д.т.н., проф. Сімоненко В.П.		

7.Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів дипломного проекту	Строк виконання етапів проекту	Примітки
	Затвердження теми роботи	*1.09.2019*	
	Вивчення та аналіз завдання	*2.09.2019-14.03.2020*	
.	*Розробка архітектури та загальної структури програми*	*14.03.2020-25.03.2020*	
.	*Розробка структур окремих Інтерфейсів програми*	*25.03.2020-2.04.2020*	
	Програмна реалізація	*2.04.2020-13.04.2020*	
	Оформлення пояснювальної	*13.04.2020-21.05.2020*	
	Захист програмного продукту	*21.05.2020 – 25.05.2020*	
	Передзахист	*26.05.2020*	
	Захист		

Студент Гліб БАЛАЦЕНКО

Керівник Олександр ДОЛГОЛЕНКО

Анотація

В бакалаврській дипломній роботі досліджені можливості технології Intel Trusted Execution Technology (Intel TXT) та реалізовані програмні засоби навчання використанню її можливостей у віртуальному навчальному середовищі Moodle. Intel TXT перевіряє середовище запуску та встановлює корінь довіри, що, в свою чергу, дозволяє програмному забезпеченню будувати ланцюжок довіри для віртуалізованих середовищ.

Реалізовано серверну платформу Moodle, що орієнтована на вивчення персоналізованої навчальної програми по використанню можливостей технологій Intel® vPro™.

Abstract

The bachelor's thesis explores the possibilities of Intel Trusted Execution Technology (Intel TXT) and implemented software tools for learning to use its capabilities in the virtual learning environment Moodle. Intel TXT tests the startup environment and establishes the root of the trust, which in turn allows the software to build a chain of trust for virtualized environments.

A Moodle server platform has been implemented, which is focused on studying a personalized training program on using the capabilities of Intel® vPro technologies.

ВІДОМІСТЬ ДИПЛОМНОГО ПРОЕКТУ

з/п	Формат	Позначення	Найменування	Кількість листів	Примітка
	А 4		Завдання на дипломний проект	2	
	А4	ІАЛЦ.467200.001 ОП	Опис проекту	1	
	А4	ІАЛЦ.467200.002 ТЗ	Технічне завдання	5	
	А4	ІАЛЦ.467200.003 ПЗ	Пояснювальна записка	75	
	А3	ІАЛЦ.467200.004 Д1	Функціональна схема	1	
	А4	ІАЛЦ.467200.005 Д2	Принципова схема алгоритму	1	
	А3	ІАЛЦ.467200.006 Д3	Структурна схема	1	

Технічне завдання

до дипломного проекту

на тему: «Програмні засоби навчання системних адміністраторів використанню можливостей технологій Intel® vPro™:Trusted Execution-Technology»

Київ – 2020

2					**ІАЛЦ.467200.002 ТЗ**			
Изм.	*Лист*	*№ докум*	*Подпись*	*Дата*				
Разраб		*Балаценко Г.І.*			Програмні засоби навчання системних адміністраторів використанню можливостей технологій Intel vPro: Trusted Execution-Technology.	*Литера*	*Лист*	*Листов*
Пров		*Долгоненко О.М.*				*у*	*1*	*5*
						НТУУ «КПІ» ФІОТ ІО-61		
Н. Контр.		*Симоненко В.П.*						
Утв								

Зміст

1. НАЙМЕНУВАННЯ І ОБЛАСТЬ ЗАСТОСУВАННЯ

Назва розробки: Програмні засоби навчання системних адміністраторів використанню можливостей технологій Intel vPro: Trusted Execution-Technology.

Область застосування: Навчання системних адміністраторів використанню можливостей технологій Intel vPro: Trusted Execution-Technology.

2. ПІДСТАВА ДЛЯ РОЗРОБКИ

Підставою для розробки є завдання на виконання роботи кваліфікаційно-освітнього рівня «бакалавр комп'ютерної інженерії», затверджене кафедрою обчислювальної техніки Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

3. МЕТА І ПРИЗНАЧЕННЯ

Метою даного проекту є дослідження можливостей технології Intel vPro: Trusted Execution-Technology та розробка програмних засобів навчання використанню можливостей цієї технології у віртуальному навчальному середовищі Moodle.

4. ДЖЕРЕЛА РОЗРОБКИ

Джерелом розробки є науково-технічна література, публікації в виданнях, довідники, публікації в Інтернеті по опису архітектури і принципу роботи Intel vPro: Trusted Execution-Technology.

5. ТЕХНІЧНІ ВИМОГИ

5.1. Вимоги до програмної моделі серверної платформи Moodle

Програмна система має мати наступний функціонал:

- Створювати лекції, тести і завдання у вбудованому редакторі;
- Запрошувати і імпортувати користувачів, об'єднувати їх в групи, записувати їх на курси;
- Переглядати статистику активності на платформі;
- Зміна дизайну, інтеграція з іншими сервісами, візуалізація звіті.

5.2 Вимоги до програмного забезпечення серверної платформи Moodle

- Операційна система Microsoft Windows Server 2019;
- Віртуальне навчальне середовище Moodle;
- Мова сценаріїв PHP;
- Працюючий сервер баз даних.

5.3 Розглянути можливість підключення до серверної платформи Moodle баз даних

- MySQL 5.6+ ;
- PostgreSQL 9.4+ ;
- MariaDB 5.5.31+ ;
- Microsoft SQL Server 2008+ ;
- Oracle Database 11.2+ ;

5.4 Вимоги до апаратного забезпечення серверної платформи Moodle

- Два процесора типу Intel Xeon;
- Оперативна пам’ять - 64 GB з можливістю розширення до 128 GB;
- Відеоадаптер – інтегрований;
- Дискові накопичувачі - 2 накопичувача не гірше, ніж *SAS 8TB 7200RPM rpm*;

- Контролер *SAS* - не менш ніж 8 каналів з можливістю побудови *RAID* 0, 1, 5, 6 и 10;
- Мережний контролер –1 *Gb/s* (2 шт. інтегровані в материнську плату); мережний контролер - 10 *Gb/s Fibre Channel* (2 шт.);
- Серверний корпус rackmount (висота – не більше 2U);
- Два блока живлення з функцією «гарячої» заміни (1 основний + 1 резервний);
- Резервування системних вентиляторів, можливість здійснення «гарячої»» заміни системних вентиляторів;
- Оптичний накопичувач - *DVD-RW*;
- Монтажний комплект – телескопічний комплект для монтажу сервера в стойку/шафу.

6. ЕТАПИ РОЗРОБКИ

Назва етапу	Дата
Вивчення джерел за тематикою роботи	10.01.2020
Розроблення і узгодження технічного завдання	20.02.2020
Моделювання структури програмного забезпечення	03.03.2020
Розробка програмного забезпечення	25.03.2020
Тестування системи	01.05.2020
Виправлення помилок	15.05.2020
Оформлення документації дипломної роботи	25.05.2020

Пояснювальна записка

до дипломного проекту

на тему: «Програмні засоби навчання системних адміністраторів використанню можливостей технологій Intel® vPro™: Trusted Execution-Technology»

Київ – 2020

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

(TXT) - Intel Trusted Execution Technology;

(AMT) - Intel Active Management Technology;

(VT-x) - Intel Virtualization Technology;

(VT-d) - Virtualization technology for directed I/O;

(DMA) - Direct memory access;

(SDN) - Software-defined networking;

(NAP) - Network Access Protection;

(WOL) - Wake-on-LAN;

(SOL) – Serial Over LAN;

(UUID) - Universally unique identifier;

(DHCP) - Dynamic Host Configuration Protocol;

(BOOTP) - Bootstrap Protocol;

(VNC) - Virtual Network Computing;

(KVM) - Kernel-based Virtual Machine;

(WLAN) - Wireless Local Area Network;

(S0) - комп'ютер увімкнено і працює;

(ISM) - Intel Standard Manageability;

(SBT) - Intel Small Business Technology;

(PCH) - Platform Controller Hub;

(SMB) - Small Medium Business;

(HW) - HardWare;

(POST) - Power On Self Test;

(TPM) - Trusted Platform Module

(PXE) - Preboot Execution Environment

(VMMs) - Virtual Machine Managers

(PCR) - Platform Configuration Registers

(SGX) - Intel® Software Guard

(AUX) – Auxiliary

(LCP) - Launch Control Policy

(MLE) - Measured Launched Environment

(TCB) - Trusted Computing Base

(NV) - Non-Volatile

(ACM) - Association for Computing Machinery

(PO) - Platform Owner

(TCG) - Test Call Generators

(MMIO) - Memory-mapped I/O

(API) - Application Programming Interface

ВСТУП

Метою даного проекту є дослідження можливостей технології Intel vPro: Trusted Execution-Technology та розробка програмних засобів навчання використанню можливостей цієї технології у віртуальному навчальному середовищі Moodle.

Технологія Intel vPro - це маркетинговий термін, використовуваний Intel для великої колекції комп'ютерних технологій. Платформа Intel® vPro ™ складається з апаратного забезпечення і технологій, які утворюють будівельні блоки для бізнес-обчислень. Специфікація платформи систематично оновлюється заради забезпечення безперервних інновацій. Кожне наступне покоління Intel® vPro ™ націлене на постачання запасу продуктивності для бізнес-процесів при одночасній реалізації гнучких форм-факторів з метою побудови різних обчислювальних середовищ.

Однією із головних технологій, що реалізовані на платформі Intel® vPro™, є Intel Trusted Execution Technology.

Технологія Intel® Trusted Execution (Intel® TXT) - це технологія, яка використовує вдосконалену архітектуру процесорів, спеціальне обладнання та прошивки, які дозволяють певним процесорам Intel забезпечити основу для багатьох нових нововведень у безпечні обчислення. Вона особливо добре підходить для хмарних обчислень та інших застосувань, коли цілісність даних є найважливішою. ЇЇ основна мета – створити середовище, якому можна довіряти з самого початку та надалі забезпечувати системне програмне забезпечення засобами для кращого захисту цілісності даних.

Існує дуже невелика кількість джерел де описані можливості цієї технології, майже всі вони є англомовними. У зв’язку з цим розробка програмних засобів навчання в системі Moodle використанню можливостей Trusted Execution-Technology – є дуже актуальною і може знайти попит на навчання у співробітників багатьох ІТ компаній.

РОЗДІЛ 1.
ОГЛЯД ТЕХНОЛОГІЇ INTEL® VPRO™

1.1 Технологія Intel® vPro ™

Технологія Intel vPro - це зонтикоподібний маркетинговий термін, який використовується Intel для назви великої колекції комп'ютерних апаратних технологій, включаючи Hyperthreading, Turbo Boost 3.0, VT-x, VT-d, Trusted Execution Technology (TXT), Intel Active Management Technology (AMT) та інші. Коли бренд vPro був запущений (близько 2007 року), він був ідентифікований головним чином з AMT, тому деякі журналісти все ще вважають AMT суттю vPro.

1.2 Функції vPro ™

Intel vPro - торговий бренд для набору апаратних функцій ПК. Комп'ютери, що підтримують vPro, в якості основних елементів мають процесор з підтримкою vPro, чіпсет з підтримкою vPro і BIOS з підтримкою vPro.

ПК vPro містить:

• Багатоядерні, багатопотокові процесори Xeon, або Core з підтримкою vPro.

• Провідне і бездротове підключення до мережі.

• Технологію Intel AMT - асортимент апаратних функцій, орієнтованих на бізнес, що дозволяють отримати віддалений доступ до ПК щоб виконати завдання по управлінню або безпеці, навіть якщо ОС не працює або вимкнено живлення ПК. Зауважте, що AMT - це зовсім не те ж саме, що Intel vPro; AMT - це тільки один елемент vPro ПК.

• Технологію Intel Virtualization, що включає Intel VT-x для процесора і пам'яті, та Intel VT-d заради введення / виведення і підтримки віртуалізованих середовищ. Intel VT-x прискорює апаратну віртуалізацію, що дозволяє формувати ізольовані регіони пам'яті заради запуску критичних додатків на апаратних віртуальних машинах з метою підвищення цілісності запущеного додатку і конфіденційності конфіденційних даних. Intel VT-d відкриває захищені адресні простори віртуальної пам'яті периферійних пристроїв DMA, підключеним до комп'ютера через шини DMA, зменшуючи загрозу, яку створюють шкідливі периферійні пристрої.

• Технологію віддаленої конфігурації для AMT з захистом на основі сертифікатів. Віддалену конфігурацію дозволено виконати на системах, навіть до встановлення ОС та/або агентів управління програмним забезпеченням.

• Технологію Intel Trusted Execution (Intel TXT), яка перевіряє середу запуску і встановлює корінь довіри, який, в свою чергу, дозволяє програмному забезпеченню створювати ланцюжок довіри для віртуалізованих середовищ. Intel TXT також захищає секрети при переході живлення як для упорядкованого, так і для безладного відключення (традиційно вразливий проміжок часу для облікових даних безпеки).

• Підтримку IEEE 802.1X, мережі самозахисту Cisco (SDN) і захисту доступу до мережі Microsoft (NAP) на ноутбуках і підтримка 802.1x і Cisco SDN на настільних ПК. Підтримка цих технологій безпеки дозволяє Intel vPro зберігати позицію безпеки ПК, для того щоб мережа могла аутентифікувати систему перед завантаженням ОС і додатків і перед тим, як ПК буде дозволений доступ до мережі.

• Біт відключення виконання (Execute disable bit), який за підтримки ОС може запобігти атакам переповнення буфера.

1.3 Віддалене управління

Intel AMT - це комбінація функцій управління і безпеки, вбудованих в vPro ПК, спрощує системному адміністратору моніторинг, обслуговування, захищеність і обслуговування ПК. Intel AMT (технологія управління) час від часу її помилково ототожнюють з Intel vPro (платформою ПК), хоча вона є лише однією з найвідоміших технологій ПК на базі Intel vPro.

Intel AMT охоплює:

Зашифроване віддалене підключення / зменшення живлення(через пробудження та локальну мережу або WOL;

Віддалене / перенаправлене завантаження (за допомогою інтегрованого перенаправлення електронного пристрою);

Перенаправлення консолі (через послідовне використання та локальну мережу або SOL)

Попереднє завантаження доступу до налаштувань BIOS;

Програмована фільтрація для вхідного і вихідного мережевого трафіку;

Відстеження присутності агента;

Застереження на основі політики за межами діапазону.

Доступ до системної інформації, такої як всеохоплюючий єдиний в своєму роді ідентифікатор ПК (UUID), відомості про апаратні засоби, стійкі журнали подій і інша інформація, яка зберігається в виділеної пам'яті (не на жорсткому диску), де вона доступна, навіть якщо ОС не працює або ПК вимкнений.

Нині апаратне керування було доступне в минулому, але воно обмежувалося автоматичною конфігурацією (для комп'ютерів, які цього

вимагають) за допомогою DHCP або BOOTP з метою динамічного розподілу IP-адреси і бездискових робочих станцій, а також заради безвідмовної локальної мережі віддалено, харчування систем.

1.4 Пульт дистанційного керування KVM на базі VNC

Починаючи з vPro, що містить AMT 6.0, всі ПК, побудовані на основі процесів i5 або i7 і вбудованої графіки Intel, містять вбудований VNC-сервер Intel. Ви можете скористатися позадіапазонним віддаленим підключенням до ПК своєї регіональної мережі, використовуючи спеціалізовану технологію перегляду, сумісну з VNC, і мати повну здатність KVM (клавіатури, відео і миші протягом всього циклу живлення- включаючи безперебійне управління робочим столом при завантаженні ОС. Такі клієнти, як VNC Viewer Plus від RealVNC, також надають додаткову функціональність, яка може полегшити здійснення (і перегляд) певних операцій Intel AMT, таких як відключення і включення до комп'ютера, налаштування BIOS та встановлення віддаленого зображення.

Не всі процесори i5 та i7 з vPro можуть підтримувати KVM. Це залежить і від параметрів BIOS OEM і наявності дискретної відеокарти. Виключно інтегрована HD-графіка Intel підтримує здатність KVM.

1.5 Бездротовий зв’язок

Intel vPro підтримує зашифрований дротовий і бездротовий зв'язок локальної мережі для всіх функцій віддаленого керування для ПК, що знаходяться всередині корпоративного брандмауера. Intel vPro підтримує зашифровану комунікацію для деяких функцій віддаленого управління для дротових і бездротових локальних ПК за межами корпоративного брандмауера.

Ноутбуки з vPro включають гігабітне мережове підключення і підтримують бездротові протоколи IEEE 802.11 a / g / n.

Комп'ютери Intel vPro підтримують бездротове взаємодії з функціями AMT.

Для бездротових ноутбуків, живляться від акумулятора, взаємодія з функціями AMT може відбуватися, коли система підключена до корпоративної мережі. Цей зв'язок доступний, навіть коли операційна система не працює, або відсутні агенти керування.

Позадіапазонна комунікація AMT і окремі функції AMT доступні для бездротових або дротових ноутбуків, підключених до корпоративної мережі через віртуальну приватну мережу (VPN) на базі ОС, якщо ноутбуки прокинулися і працюють належним чином.

Бездротове з'єднання працює на двох рівнях: інтерфейс бездротової мережі (WLAN) і драйвер інтерфейсу, який виконується на хості платформи. Мережевий інтерфейс керує зв'язком радіочастотного зв'язку.

Коли користувач вимикає бездротової передавач / приймач за допомогою апаратного перемикача, Intel AMT не може використовувати бездротовий інтерфейс ні за яких умов, поки користувач не включить бездротової передавач / приймач.

Intel AMT Release 2.5 / 2.6 дозволяє відправляти і отримувати трафік управління через WLAN виключно тоді, коли платформа знаходиться в режимі живлення S0 (комп'ютер включений і працює). Він не отримує бездротової трафік, коли хост спить або вимикається. Якщо стан живлення дозволяє, Intel AMT Release 2.5 / 2.6 може продовжувати відправляти та одержувати позаполосний трафік, якщо платформа знаходиться в стані Sx, але лише за допомогою дротового з’єднання локальної мережі, якщо така існує.

Версія 4.0 і пізніші версій підтримують можливість керування бездротовим бездіапазонним режимом в станах Sx, в залежності через налаштування живлення та інших параметрів конфігурації.

Випуск 7.0 підтримує контрольованість бездротовим зв'язком на настільних платформах.

Коли бездротове з'єднання встановлено на хост-платформі, воно базується на бездротовому профілі, який встановлює імена, паролі та інші елементи захисту, які використовуються з метою аутентифікації платформи до бездротової точки доступу. Користувач або IT-формування визначає один або кілька профілів за допомогою інструменту, такого як Intel PROSet / Wireless Software. У випуску 2.5 / 6 Intel AMT повинна буда мати у своєму розпорядженні відповідний бездротовой профіль для отримання позадіапазонного по тому ж бездротовому каналу зв'язку. API мережевого інтерфейсу дозволяє визначати один або кілька бездротових профілів, використовуючи ті ж параметри, що і програмне забезпечення Intel PROSet / Wireless. Під час живлення хоста Intel AMT спілкується з драйвером мережі WLAN на хості. Коли драйвер і Intel AMT знаходять відповідні профілі, драйвер направляє трафік, адресований пристрої Intel AMT заради обробки керованості. З певними обмеженнями, Intel AMT Release 4.0 / 1 може посилати і приймати позаполосній трафік не беручи до уваги бездротового профілю, налаштованого Intel AMT, якщо активний драйвер хоста і платформа знаходиться в середині підприємства.

У версії 4.2 і на версії 6.0 бездротових платформ WLAN включений за замовчуванням як до, так і після конфігурації. Це означає, що дозволяється налаштувати Intel AMT через WLAN, поки у головного драйвера WLAN є активне з'єднання. Intel AMT синхронізується з активним профілем хоста. Він передбачає, що сервер конфігурації налаштовує бездротової профіль, Intel AMT використовує в станах харчування, відмінних від S0.

Якщо виникає складне становище з драйвером бездротового зв'язку, а хост все ще працює (тільки в режимі живлення S0), Intel AMT може продовжувати приймати трафік управління в межах дії безпосередньо з інтерфейсу бездротової мережі.

Щоб Intel AMT працював з бездротовою локальною мережею, він повинен розподілятися IP-адресами з хостом. Це вимагає наявності сервера DHCP для розподілу IP-адреса, а Intel AMT повинен бути налаштований для використання DHCP.

1.6 Зашифрований зв’язок під час роумінгу

Пк Intel vPro підтримують зашифровану взаємодія у роумінгу. vPro комп'ютер версії 4.0 або більше підтримує охорону моб. зв'язку лінією визначення захищеного тунелю з метою зашифрованого взаємозв'язку AMT з контрольованим постачальником послуг у роумінгу (функціонує у відкритій, дротовій локальній мережі за межами корпоративного брандмауера). Безпечне спілкування з AMT можливо визначити, в разі якщо портативний комп'ютер вимкнений або ОС відключена. Закодований тунель зв'язку AMT винайдений подібним способом, для того щоб системним адміністраторам можна було отримати доступ до ноутбука або настільного комп'ютера у супутникових кабінетах, в якому відсутні проксі-сервера або прилади сервера управління.

Нешкідливі комунікації за межами колективного брандмауера знаходяться в залежності від додавання до мережевої інфраструктури новітнього компонента - сервера наявності управління (Intel іменує це "шлюзом з допомогою vPro"). Для цього потрібна інтеграція з виробниками мережевих комутаторів, постачальниками брандмауерів та постачальниками, які розробляють консолі управління з метою формування інфраструктури, які утримують зашифровані роумінгові комунікації. Таким чином, хоча зашифрований роумінговий зв’язок увімкнено як функцію в vPro ПК версії 4.0 і новіших, ця функція не буде повною мірою працювати, поки інфраструктура не буде створена і не запрацює.

1.7 vPro безпека

Технологічні процеси та методології vPro захищеності підтримуються чіпсетом комп'ютера та іншим системним оснащенням. В період розгортання комп'ютера vPro, облікові відомості захищеності, ключі та інша суттєві відомості зберігаються та оберігаються в захищеній пам'яті (не в жорсткому диску) також стираються, якщо вони більше не потрібні.

1.8 Питання безпеки та конфіденційності

Згідно з відомостями Intel, вимкнути AMT можливо за допомогою опції BIOS, але, ймовірно, більшість користувачів ніяк не можуть виявити зовнішній допуск до свого комп'ютер із підтримкою апаратної технології vPro. Більш цього, процесори з мікроархітектурою Sandy Bridge та подальші чіпи мають "... ймовірність дистанційного знищення та відновлення розгубленого або вкраденого комп'ютера за допомогою 3G".

У травні 2017 року Intel розмістила поради щодо захищеності уразливості мікропрограмного забезпечення в певних системах, що використовують Intel AMT, Intel Standard Manageability (Intel ISM) або Intel Small Business Technology (Intel SBT). Незахищеність ймовірно вважається досить значною бо може надати ймовірність правопорушнику віддалено отримати допуск до бізнес-комп'ютера та робочих станцій, що використовують дані технологічні процеси. Фірма Intel радить людям та фірмам, що використовують бізнес-комп'ютери та прилади, в які, інтегровані Intel AMT, Intel ISM або Intel SBT, використовувати оновлення мікропрограмного забезпечення від виготовлювача оснащення, якщо це допустимо, або дотримуватися крокі, що приводять до пом'якшення результатів атак.

Численні функції vPro, в тому числі AMT, реалізовані у Intel Management Engine (ME), окремому процесорі в північному мості чіпсету, що

входить до складу сучасних головних проесорів та управляється окремою спеціальної ОС MINIX 3. ME, як було виявлено, володіє багатьма уразливостями у захищеності. Конструктивно ME представляє собою 32-розрядний процесор з архітектурою x86. Цей процесор завжди працює, навіть коли виключено живлення. Живиться він від батарейки на материнській платі, а його ОС MINIX 3 знаходиться в енергонезалежній пам'яті, що входить до складу північного мосту. Методу відключення ME не існує – цей процесор завжди увімкнений і готовий до роботи, якщо він не вимкнений OEM виробником.

1.9 Особливості безпеки

Intel vPro підтримує стандартні галузеві методології та протоколи, а також інші функції безпеки постачальників:

- Industry-standard Trusted Platform Module version 1.2 (TPM);
- Support for IEEE 802.1x, Preboot Execution Environment (PXE), and Cisco Self Defending Network (SDN) in desktop PCs, and additionally Microsoft Network Access Protection (NAP) in laptops;
- *Execute Disable Bit*;
- *Intel Virtualization Technology (Intel VT(Vt-x+Vt-d))*;
- *Intel VMCS-Intel Virtual Machine Control Structure Shadowing*;
- *Intel Platform Trust Technology-PTT*;
- *Intel Data Protection Technology*;
- *Intel Identity Protection technology*;
- *Intel Secure key*;
- *Intel Anti-Theft Technology*;
- *Intel Boot Guard*;
- *Intel OS Guard*;
- *Intel Active Management Technology-Intel AMT*;
- *Intel Stable Image Platform Program-SIPP*;
- *Intel Small Business Advantage-Intel SBA*;

- *Intel Trusted Execution*;
- *Technology (Intel TXT).*

1.10 Intel Boot Guard

Intel Boot Guard - це процесорна апаратна функція, або технологія, що перешкоджає здійснювати загрузку ПК від несанкціонованої модифікації програмних модулів UEFI. Модулі, що загружаються, повинні мати цифровий підпис Intel або виробника ПК. Ці підписи перевіряються при кожній загрузці. Як результат, Intel Boot Guard не дає остаточним користувачам можливості заміни інтегрованих програмних продуктів. Технологія Boot Guard була вперше реалізована в процесорах Intel Core четвертого покоління (Haswell).

1.11 Технології та методології

Intel vPro використовує ряд стандартних технологій і методологій безпеки з метою захисту віддаленого каналу зв'язку vPro. Ці технології і методології в свою чергу покращують захищеність доступу до критичних системних даних ПК, налаштувань BIOS, функції управління Intel AMT і інших чутливих функцій або даних та оберігають облікові дані і іншу важливу інформацію в період розгортання (налаштування і конфігурації Intel AMT) і використання vPro.

Intel vPro використовує також протокол безпеки транспортного рівня (TLS), в тому числі загальнодоступний ключ TLS (TLS-PSK) з метою захисту зв'язку через поза діапазонний мережевий інтерфейс. Здійснення TLS використовує 128-бітове кодування AES і ключі RSA з довжиною модуля 2048 біт.

Протокол аутентифікації дайджесту HTTP, відповідає вимогам RFC 2617. Консоль керування перевірки справжності IT-адміністраторів, керуючих ПК на Intel AMT:

• Одноразовий вхід на Intel AMT за допомогою аутентифікації домену Microsoft Windows на основі протоколів Microsoft Active Directory і Kerberos.

• Генератор псевдовипадкових чисел (PRNG) в прошивці ПК AMT, що генерує якісні сеансові ключі з метою безпечного зв'язку.

• Завантажуватися і виконуватися можуть лише зображення цифрового програмного забезпечення (підписані Intel).

• Збереження критичних даних, у захищеному вигляді від несанкціонованого доступу, за допомогою захищеного, стійкого (незалежного) сховища даних в апаратному забезпеченні Intel AMT.

• Списки контролю доступу до діапазону Intel AMT та інших функцій управління.

1.12 Можливості технології vPro в умовах SMB та Enterprise компанії

Технологія vPro набагато розширює потенціал щодо управлінням парком ПК в умовах сучасної компанії, до того ж так само як малий (SMB - small medium business), так і великий (enterprise). Технологія дозволяє зменшити кількість викликів технічних фахівців на робочі місця користувачів, так більшу частину завдань, відповідно до vPro, можливо вирішувати віддалено. Інтегрувати технологію vPro можливо в уже існуючу IT-інфраструктуру, безсумнівно з поправкою на те, що потенціал технології буде застосовно тільки для ПК з підтримкою vPro.

З метою відповідати технології vPro комп'ютер зобов'язаний неодмінно відповідати наступним вимогам:

• Процесори Intel Core i5 і Core i7 з підтримкою технології віртуалізації;

• Системна логіка Intel Q77;

• Гігабітний мережевий адаптер Intel (82578DM) з підтримкою технології Intel Active Management 6.

Технологія vPro використовує власну підмережу для керування комп'ютерами, при цьому з'єднання забезпечується за існуючої фізичної інфраструктурою. Системний BIOS ПК з підтримкою vPro охоплює розширений розділ зі спеціальним ПО, яке дозволяє або отримувати IP-адресу від DHCP сервера (крім участі ОС на ПК) або поставити його вручну. Адміністрування vPro-ПК може втілюватися в дійсність аж ніяк не лише при працюючому ПК, але і на ПК, що знаходиться в сплячому або вимкненому (!) стані. Це, зокрема, дозволяє вести всі сервісні роботи з комп'ютерами користувачів після закінчення робочого дня і виключення простоїв.

Технологія vPro передбачає два основних рівня свого використання:

1. Режим SMB;

2. Режим Enterprise.

1.13 Режим SMB

Застосовується в малому бізнесі. Заради базової функціональності та не вимагає додаткових витрат на придбання спеціального ПО з підтримкою технології vPro. При такому сценарії використання забезпечуються такі функції:

• Віддалене регулювання живлення;

• Перегляд даних про основне обладнання (інвентаризація);

• Перегляд енергонезалежного журналу подій;

• Віддалене реконструювання AMT Firmware;

• Вбудований апаратний KVM.

Встановлений функціонал забезпечується простим управлінням з консолі управління до клієнта vPro за допомогою web-інтерфейс на порт 16992 (див. Рис. 1.1 і рис. 1.2):

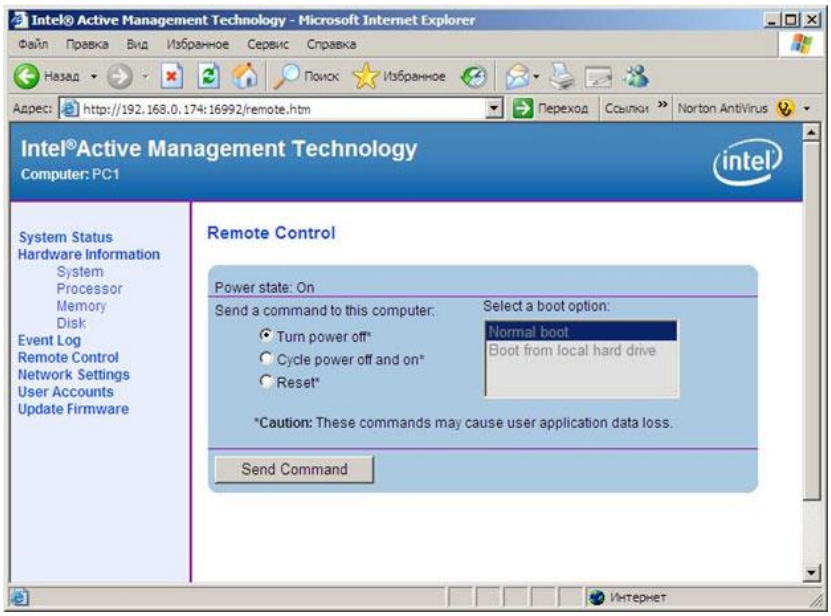


Рис. 1.1– Дистанційне керування

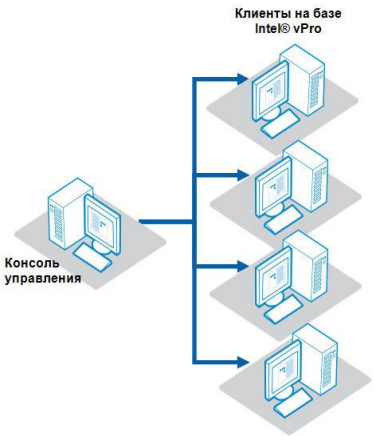


Рис. 1.2 – Консоль управління

При використанні додаткового ПЗ (Система централізованого управління з підтримкою AMT: SyAM Desktop Monitor Local + SyAM Server Monitor Central або LANDesk Management Suite) функціональність рішення набагато зростає:

• Налаштування системи оповіщення на основі апаратних датчиків платформи (оповіщення про несправності устаткування, зависання ОС і т. П);

• Віддалене завантаження (IDE посилання) - завантаження vPro-клієнта в носій на сервері. Ця функція може бути використана, зокрема, в разі неможливості завантажити ОС на клієнтському комп'ютері, в тому числі не забороняється вдатися чинним на сервері для відновлення і діагностики (див. Рис. 1.3);

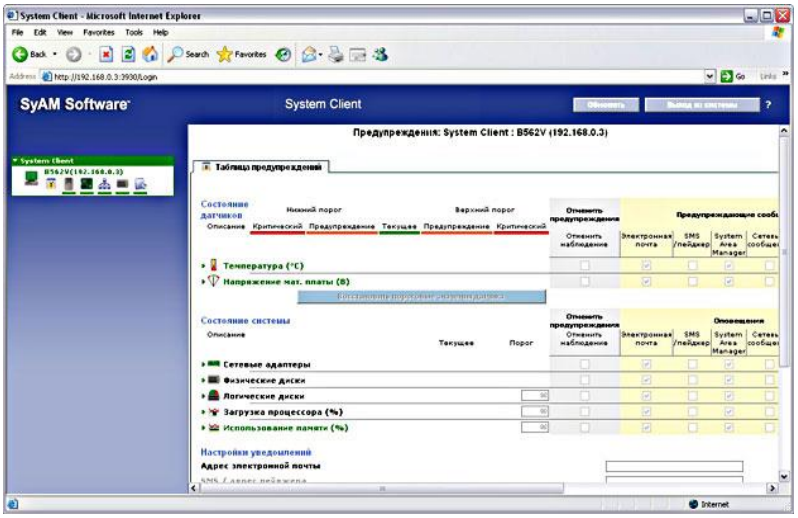


Рис. 1.3 – Таблиця попереджень

• Переадресація консолі функція SOL (Serial-over-LAN) - призначена з метою переправлення текстової консолі з робочої станції на центральну консоль управління. В рамках SOL-сесії можливий віддалений доступ до BIOS і експлуатація з текстовими операційними системами і додатками;

• Моніторинг агента керування;

• Оборона системи: a). фільтрування вхідного і вихідного трафіку ОС (вбудовані апаратні фільтри заради перевірки усередині смугового і неполісного мережевого трафіку) b). ізольованість заражених ПК (апаратна блокування мережевого трафіку)

• Оновлення антивірусної і анти шпигунського ПЗ в віддаленому режимі (див. Рис. 1.4);

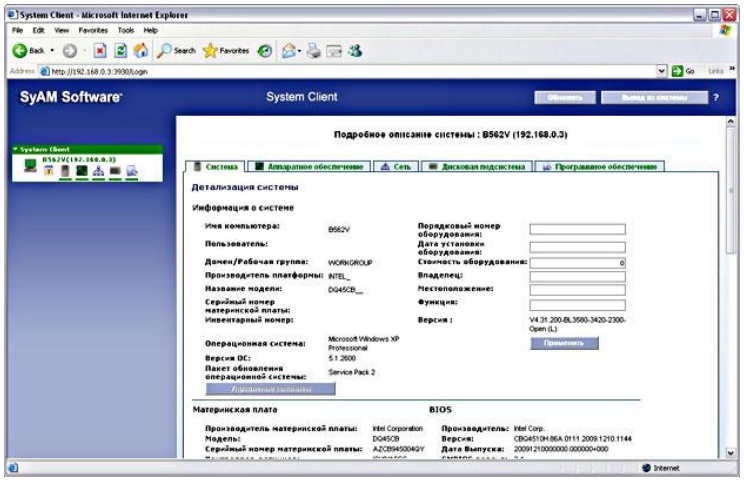


Рис. 1.4 – Опис системи

Значна кількість функцій vPro в режимі SMB зараз дозволено експлуатувати за допомогою безкоштовної утиліти Intel System Defence Utility, яка комплектується на всіх ПК Team Office b583V (див. Рис. 1.5, 1.6, 1.7).

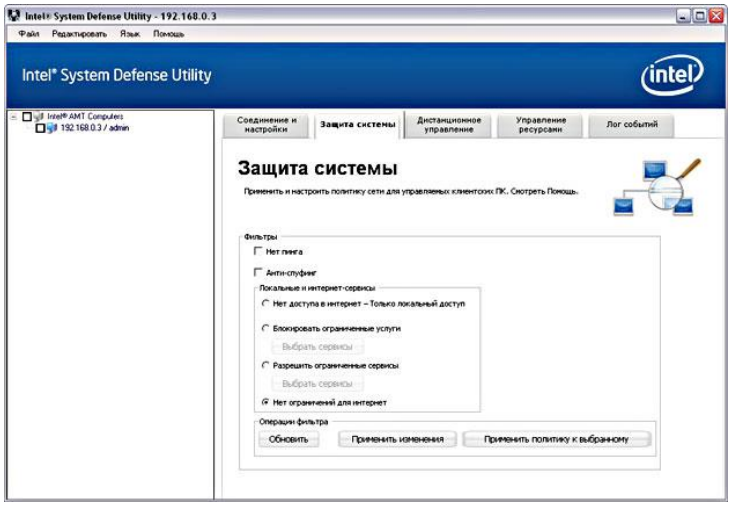


Рис. 1.5 – Захист системи

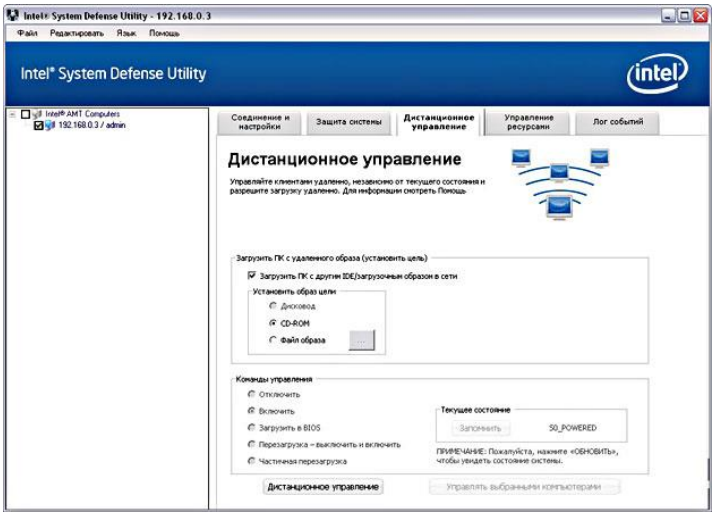


Рис. 1.6 – Дистанційне керування

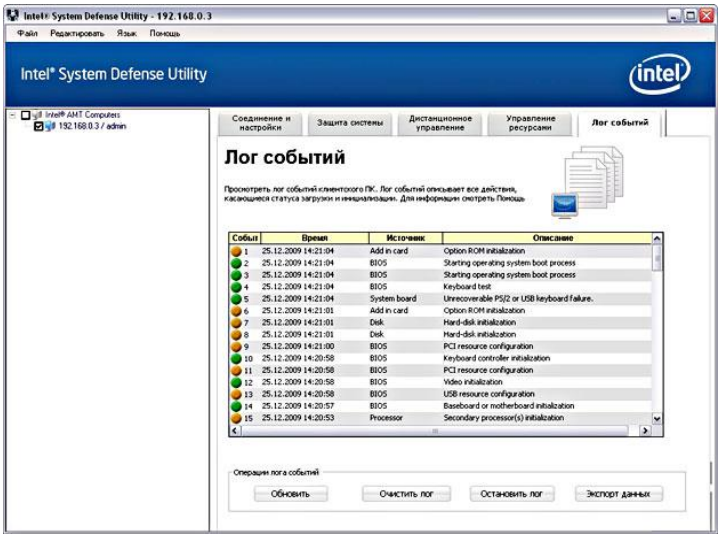


Рис. 1.7 – Лог подій

1.14 Режим Enterprise

В цьому режимі з заради кожної vPro-системи створюється винятковий аккаунт, генеруються ключі безпеки, після переносяться на клієнтські ПК на медіа носіях (USB-flash). Далі адміністрування клієнтів здійснимо всього-на-всього після взаємної аутентифікації і конфігурації. При використанні технології vPro в режимі enterprise використовуються протоколи шифрування TLS w / AES 128-bit або TLS w / RC4 128-bit, який набагато підвищує ступінь безпеки.

Режим Enterprise рекомендується з метою великих підприємств, тому що припускає велику копіткість і труднощі в розгортанні.

Внаслідок технології vPro спрощується шанс адміністрування парку ПК сервісною службою, яка знаходиться за межами організації(див. Рис. 1.8):

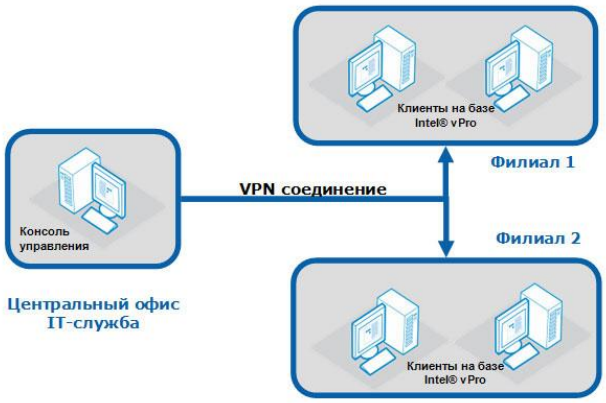


Рис. 1.8 – Парк ПК сервісної служби

Таким чином, інтегровані програмно-апаратні засоби vPro дозволяють централізовано обчислювати завдання в двох основних напрямках:

1. Керівництво:

• Віддалене завантаження з консолі управління;

• Віддалене регулювання ПК, хоч при відсутності агентів управління;

• Енергонезалежний журнал подій (event log)

• Функції Serial over LAN і IDE-перенаправлення;

• Настроювана гнучка система оповіщень на основі апаратних датчиків платформи (повідомлення про несправності устаткування, зависання ОС і т. П)

2. Надійність:

• Фільтрування вхідного і вихідного трафіку ОС;

• Ізолювання заражених ПК;

• Оновлення антивірусної і анти шпигунського ПЗ в віддаленому режимі.

Ціна ліцензії SyAM System Area Manager на сервер, що дозволяє виконати потенціал vPro в розширеному обсязі, становить $ 179 і $ 39 на окремий настільний ПК. Собівартість альтернативного продукту LAN Desk Management Suite 105 $ на одиночний керований пристрій.

Нехай навіть крім придбання спеціалізованого ПЗ (системи централізованого управління з підтримкою iAMT) абонент комп'ютера Team Office b583V може використовувати в своїх інтересах перевагами технології vPro моментально "з коробки": в комплект поставки b583V входить пробна 14-ти денна модифікація SyAM System Area Manager (+ Client & Utilities), яка дозволяє дати оцінку потенціалу розширеного функціоналу vPro. Заради тих же користувачів, які в поточний момент не планують пускати в справу технологію vPro, її сприяння буде приємним "доважком", аж ніяк не збільшує цінність Team Office b583V.

Технологія Intel vPro на ПК дозволяє усунути навантаження на технічних фахівців через потенціал віддаленого моніторингу, діагностики та відновлення ПК навіть якщо в ситуаціях, якщо комп'ютер вимкнений або на ньому далеко не працює операційна система. Крім того, пересилання IT-інфраструктури на ПК з підтримкою vPro допоможе уникнути збільшення витрат, пов'язаних з підтримкою старого програмного і апаратного забезпечення, а в свою чергу звільнити час простоїв системи. Нова енергоефективна структура дозволяє зменшувати витрати на електроенергію, а вбудовані засоби захисту допомагають зменшити витрати на видалення загроз безпеці.**[1]**

ВИСНОВОК ДО РОЗДІЛУ 1

В цьому розділі були досліджені можливості технологій Intel® vPro™. Це платформа, що інтегрована в найновіші процесори фірми Intel. Вміле використання цієї платформи може забезпечити продуктивність бізнес-класу, апаратні засоби безпеки, сучасні можливості дистанційного керування та стабільність роботи.

РОЗДІЛ 2.
РОЗРОБКА СЕРВЕРНОЇ ПЛАТФОРМИ MOODLE

2.1. Що таке MOODLE?

Moodle (*Modular Object-Oriented Dynamic Learning Environment*, вимовляється «Мудл») - це модульне об’єктно-орієнтоване динамічне навчальне середовище, яке називають також системою управління навчанням, системою управління курсами, віртуальним навчальним середовищем або просто платформою для навчання, яка надає викладачам, учням та адміністраторам великий набір інструментів для комп’ютеризованого навчання, в тому числі дистанційного.

Тобто, ця платформа містить велику кількість різноманітних навчальних елементів (так званих «модулів»), які забезпечують діалог та співпрацю між викладачем та студентами. За допомогою платформи викладач може обирати будь-який з модулів, розміщувати його на сайті, редагувати, оновлювати, використовувати для інформування, навчання та оцінювання студентів. Платформа дозволяє використовувати в межах навчальної дисципліни форуми, слідкувати за активністю студентів, містить зручний для користування електронний журнал оцінок.

Moodle можна використовувати не лише в навчанні школярів, студентів, але також при підвищенні кваліфікації, бізнес-навчанні тощо.

Moodle – це безкоштовна система, яка не потребує для своєї роботи жодного платного програмного забезпечення.

Обмежень щодо використання Moodle немає. Цю систему можна встановити на домашньому комп’ютері, в локальній мережі навчального закладу та глобальній мережі Інтернет.

2.2. Чи складно навчитися користуватися Moodle?

Навчитись використовувати Moodle самостійно нескладно. Для впевненого користувача комп'ютера система проста і зрозуміла навіть на інтуїтивному рівні. Однак не зашкодить детальніше ознайомитися з її особливостями за допомогою спеціальної літератури та інтернет-ресурсів. Найкращим ресурсом є сайт Moodle, де можна знайти та завантажити навчальні матеріали українською мовою, наприклад про те встановити Moodle на персональний комп'ютер, безкоштовно завантажити посібник для роботи з Moodle та ін. Для тих, хто добре володіє англійською мовою корисною буде книга Moodle for dummies («Мудл для початківців»), у якій просто і доступно пояснюються основні особливості роботи з цією платформою.

2.3. Як створити курс Moodle?

Для того, щоб створити курс достатньо увійти в Moodle та натиснути кнопку «Додати новий курс». В університетах є багато факультетів, тому процедура створення курсу буде складнішою. Зазвичай потрібно скористатись кнопкою «керування курсом», тоді відкриється перелік факультетів і кафедр. У цьому переліку потрібно буде знайти свій факультет і кафедру, а тоді вже скористатись кнопкою «Додати новий курс».

Після цього відкриється вікно з параметрами курсу, які необхідно заповнити.

Всі параметри поділені на групи:

- загальне;
- опис;
- формат курсу;
- вигляд;
- файли і завантаження;
- доступ для гостя;
- групи;

• перейменування ролі.

• Особливої уваги заслуговує параметр «формат курсу», завдяки якому буде відображатися його зміст. Є чотири види формату курсу:

• тижневий – використовується, якщо навчання на курсі організовується потижнево, з точною датою початку та кінця, чітко визначеними строками;

• тематичний – розділяє курс на теми. Такий формат зручний для курсів, які тривають протягом семестру або навчального року;

• форумний формат – навчання проходить у вигляді форуму, який може оцінювати викладач;

• формат єдиної діяльності – на сторінці курсу буде показано тільки один елемент або ресурс.

2.4. Скільки часу займає розробка електронного курсу в Moodle?

Час необхідний для розробки навчального курсу в Moodle залежить від цілей та пріоритетів, які ставить перед собою розробник. Якщо є потреба у розробці повноцінного складного курсу, який буде включати лекційний матеріал, плани практичних занять, електронні ресурси, матеріали для самостійної роботи, тестові завдання тощо, то розробка може зайняти досить багато часу – від кількох тижнів (якщо є готові напрацювання, які здебільшого можна скопіювати), до кількох місяців (якщо усі матеріали потрібно розробляти з нуля).

У випадку обмеженого часу, коли потрібно швидко організувати дистанційне навчання, можна створити спрощений варіант курсу, робота над яким триватиме від кількох годин до кількох днів. При цьому не обов’язково одразу розміщувати усі модулі, спочатку достатньо розмістити лише найважливіші, які дозволяють надавати студентам навчальний матеріал та оцінювати їхню роботу. Кількість модулів у курсі можна поступово збільшувати, їхній зміст ускладнювати, змінювати способи оцінювання студентів та ін.

Позитивною рисою платформи є те, що модуль можна «приховати» на той час, поки він не завершений. У такому випадку його буде бачити лише викладач. Також модулі по наступних темах можна приховувати до тих пір, поки студенти не виконають завдання з попередніх тем. І лише після цього зробити їх видимими.

2.5. За допомогою яких модулів відбувається співпраця викладача з студентом?

Співпраця викладача зі студентами відбувається за допомогою двох типів модулів: «Види діяльності» та «Ресурси». Перша група модулів – *види діяльності* – передбачає можливість створення завдань для оцінювання студентів. Ці об'єкти надають можливості для спілкування зі студентами (наприклад, об'єкти «Форум», «Чат», «Зворотній зв'язок»), їхнього тестування (модуль «Тести»), виконання завдань, що передбачають завантаження файлів з результатами роботи (наприклад, модулі «завдання» чи «семінар»), розміщення елементів для спільної роботи (модуль «Вікі») та ін.

Ресурс у системі Moodle – це група об'єктів, які дозволяють додати до курсу будь-який вміст. Наприклад, це можуть бути веб-сторінки, текстові сторінки, написи, посилання на файли (модуль «Файл»), веб-сторінки (модуль «URL-веб посилання»), каталог із файлами (модуль «Тека»), текстові сторінки у форматі книги (модуль «Книга»).

Викладач сам обирає, які з цих об'єктів розміщувати на курсі, виходячи з мети та завдань навчальної дисципліни. **[2]**

2.6. Як встановити Moodle на локальний комп'ютер

Moodle - переважно серверна платформа. Тільки сервер дозволяє без обмежень реалізувати весь потенціал системи, якщо не брати до уваги платні хостинги. У сервера сховище обмежена лише вашим місцем на диску, можна запрошувати скільки завгодно користувачів і впроваджувати будь-які розробки.

Перед установкою потрібно переконатися, що комп'ютер відповідає мінімальним вимогам (див табл. 2.1):

Таблиця 2.1 – Мінімальні вимоги до ПК при встановленні Moodle

Мінімальні вимоги до сервера:	Встановленні наступні бази даних:
Процессор: 2-х ядерный, 2ГГц ОЗУ: 1ГБ Місце на диску: 5ГБ	MySQL 5.6+ PostgreSQL 9.4+ MariaDB 5.5.31+ Microsoft SQL Server 2008+ Oracle Database 11.2+

Серверний формат підійде компаніям і установам, які хочуть створити локальне простір для навчання без інтернету. До такої Moodle зможуть підключитися лише користувачі з локальної мережі комп'ютера, на який встановлена система.

2.7. Що треба зробити для установки

Крок 1. Скачайте діструбітів Moodle

Установчий пакет можна завантажити з сайту Moodle. Всі версії можна знайти в розділі Downloads, підтримується як Windows, так і Mac OS. Безпечніше буде вибрати останню стабільну версію (Stable). Так ви завантажте інсталяційний архів на свій комп'ютер.

Крок 2. Розархівуйте дистрибутив окрему папку

Система готова до установки, але перед цим варто підготувати папку для файлів системи. Так ви зможете зберігати всі файли Moodle в одному місці. Створивши папку, розархівуйте архів в неї.

Крок 3. Запустіть інсталятор

Запустіть Start Moodle.exe. Це відкриє cmd-вікно (інтерпретатор командного рядка Windows), і система зробить попередню настройку, як показано на рис. 2.1.

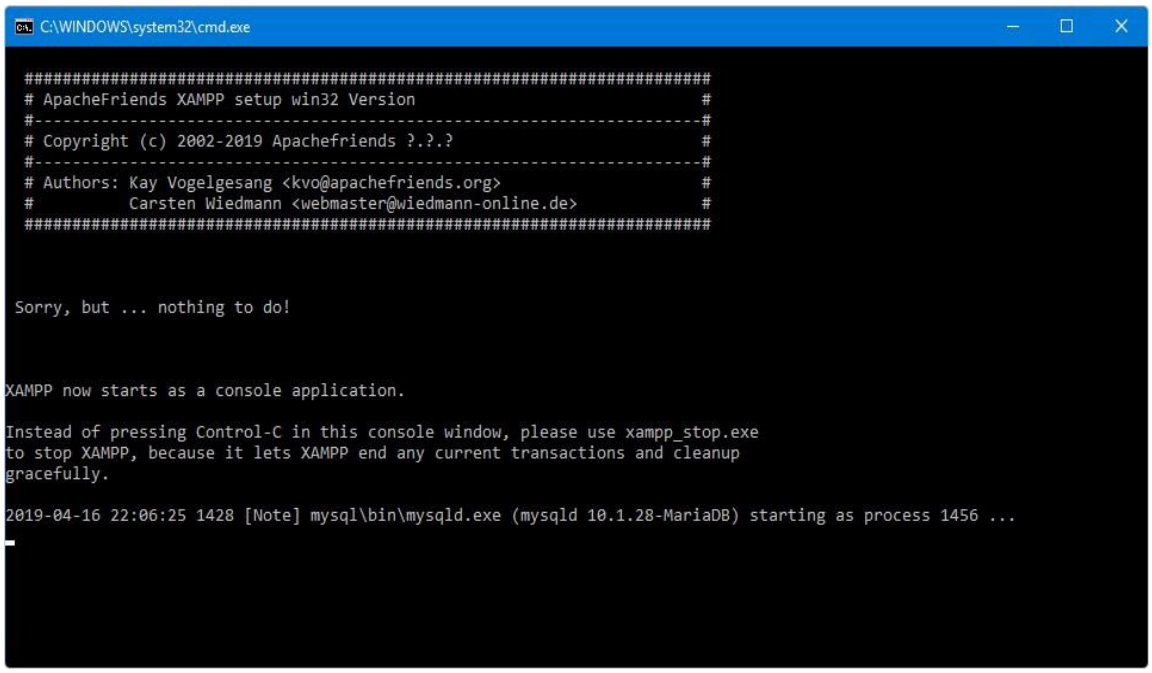


Рис. 2.1 – Вигляд cmd вікна(інтерпретатор віндовс)

Крок 4. Відкрийте Moodle в браузері

Працювати в Moodle ви будете через браузер. Відкрийте улюблений браузер і наберіть localhost: це універсальний локальну адресу вашого комп'ютера, для цього не потрібно підключення до інтернету.

Крок 5. Встановіть Moodle

Встановіть Moodle, виконуючи вказівки в керівництві. Вас попросять придумати пароль і назву для бази даних, потім база даних почне генеруватися, а в кінці буде потрібно створити ім'я та пароль адміністратора, який стане першим користувачем платформи.

Moodle готова до роботи.

2.8. Що може початкова версія

Після установки ви потрапляєте на початкову сторінку Moodle. Це «нульова» система. Тут вже є деякі модулі, що дозволяють здійснювати базові дії, на кшталт створення курсів і записи користувачів, так що з нею вже можна працювати (див. рис. 2.2).

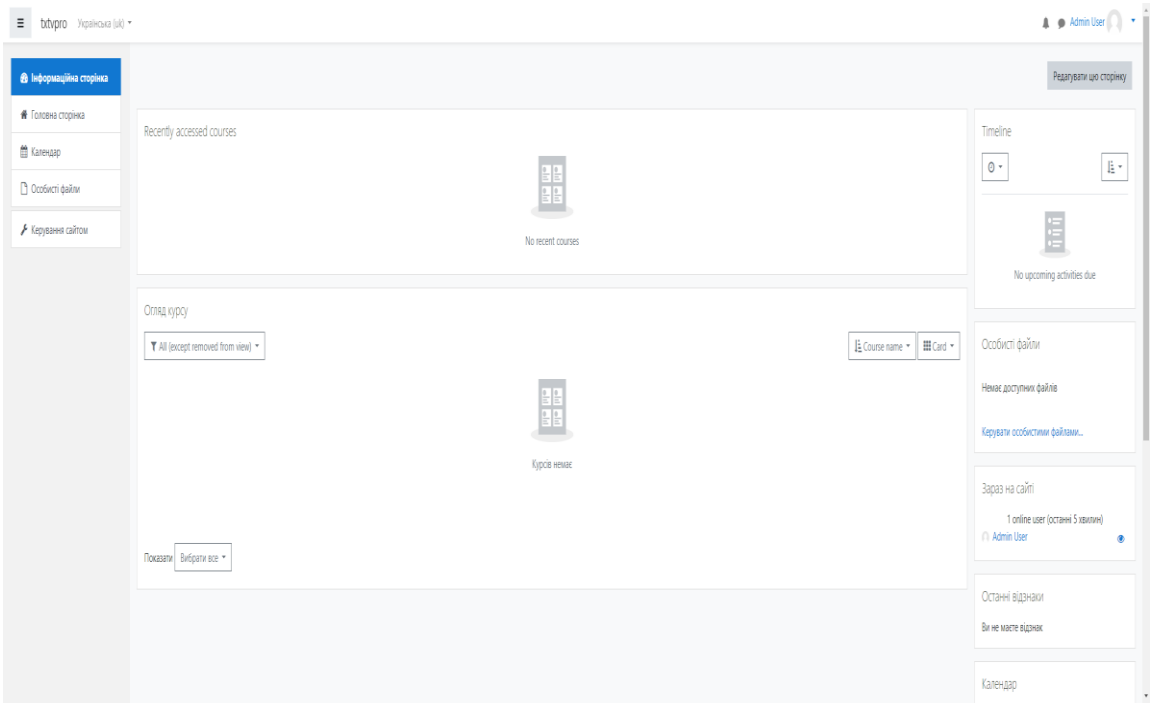


Рис. 2.2 – Початкова сторінка Moodle.

Moodle повністю управляється через панель «Адміністрування». Функцій тут не так багато, але достатньо для першого встановлення. У «нульовий» Moodle можна:

- Створювати лекції, тести і завдання у вбудованому редакторі
- Запрошувати і імпортувати користувачів, об'єднувати їх в групи, записувати їх на курси
- Переглядати статистику активності на платформі

Зміна дизайну, інтеграція з іншими сервісами, візуалізація звітів та інші функції настроюються за допомогою плагінів. Це архіви з настройками, які викачуються з інтернету і встановлюються на платформу. Наприклад, можна

додати можливість влаштовувати вебінари, чого в «нульовий» Moodle немає.**[3]**

2.9 Розробка серверної платформи для встановлення веб-серверу Moodle.

Можливі два підходи до розміщення веб серверу Moodle: використовувати або власний веб сервер, або ж розмістити його на хостингу. Розміщення на хостингу це більш дешевий варіант, але якщо у організації чи компанії є потреба в розміщені також і інших серверів, крім сервера Moodle, то більш доцільним і солідним є використання власного сервера.

За допомогою спеціального ПЗ в сервер можливо перетворити любий ПК. Таким шляхом зазвичай і обмежуються невеликі організації. З ростом популярності веб ресурсу і збільшенням його користувачів в Інтернет все замітніше будуть обмеження такого технічного рішення. У зв'язку з цим, для розгортання веб серверу Moodle є більш доцільним використання спеціалізованого комп'ютера, в котрому для якісного функціонування інформаційної системи в масштабі Інтернет використовується ряд особливих рішень. Такими рішеннями є, відмовостійкість, масштабованість, підвищена надійність та функціональне керування. Тільки повноцінний сервер може забезпечити одночасне і швидке обслуговування великої кількості користувачів.

Неможливо розробити сервер, котрий міг би задовільнити одночасно велику кількість його потенційних користувачів, бо в залежності від фінансового стану компанії, вона може виставляти різні вимоги до основних характеристик сервера. У зв'язку з цим було прийнято рішення розробити не сервер, а серверну платформу.

Серверна платформа - це рішення сервера, що має максимально можливу гнучкість. Її корпус повинен не тільки мати стоїчне виконання, але також мати максимально можливу гнучкість по встановленню всіх необхідних компонентів на визначені для них місця. При цьому блок

живлення повинен відрізнятися підвищеною надійністю та широким розкидом параметрів по електричній мережі. Оптимальним чином повинна бути продумана вентиляція корпусу.

Відносно до ТЗ, сформуємо завдання по розробці серверної платформи таким чином, щоб серверна платформа могла задовільнити як найбільшу кількість потенційних користувачів:

- Вибрати необхідне обладнання для збирання сервера в наступному складі: 2 процесора типу Intel Xeon; оперативна пам’ять - 64 GB з можливістю розширення до 128 GB; відеоадаптер – інтегрований; дискові накопичувачі - не гірше, ніж SAS 4TB 7200RPM rpm; контролер SAS - не менш ніж 8 каналів з можливістю побудови RAID 0, 1, 5, 6 и 10; мережний контролер –1 Gb/s; серверний корпус rackmount (висота – не більше 2U); два блока живлення з функцією «гарячої» заміни (1 основний + 1 резервний); резервування системних вентиляторів, можливість здійснення «гарячої»» заміни системних вентиляторів; монтажний комплект – телескопічний комплект для монтажу сервера в стойку/шафу.
- Виконати розрахунок потрібної потужності блоків живлення.

Основою розроблюваної платформи є процесори та материнська плата. Найсучаснішим рішенням є використання нового сімейства серверних процесорів фірми Intel: Xeon Gen 2 Bronze, Silver, Gold, або Platinum. В якості материнської плати була вибрана Lenovo ThinkSystem SR650 Server (Xeon SP Gen 2), що може містити 2 таких процесори. Вона продається, як окремо, так і вже вбудованою в серверний корпус Lenovo ThinkSystem SR650. Все обладнання серверної платформи зведено в табл. 2.2.

Таблиця 2.2 – Обладнання серверної платформи.

Тип компонента	Назва	TDP,	Ціна (у. о.)
Процесори	2 x Xeon Gen 2 Bronze, Silver, Gold, або Platinum: • Від 16 до 56 ядер (з частотою від 1.9 GHz до 4.5 GHz); • Кількість потоків від 32 до 112; • Загальний розмір кеш LLC 22MB -77MB.	170 - 330 W	600-7900
Материнська плата	Lenovo ThinkSystem SR650 Server (Xeon SP Gen 2) • RAID 0/1/10/5/50/6/60	60W	790
Оперативна пам’ять	4, 8 x 16GB Optane 2666 MT/s, DDR4	4,8 - 9,6 W	1260-2520
Дискові накопичувачі	2, 4, 6, 8 x Dell 2.4TB 10K RPM SAS 12Gbps 512e 2.5in Hot-plug Hard Drive	7.8 W x 2, 4, 6, 8	1412-11296
Корпус	Lenovo ThinkSystem SR650 2U	-	1200
Блоки живлення	2x hot swap/redundant 750W PLUS Platinum	-	300
Кулери	6x be quiet! BL067	15 W	180
Операційна система	Microsoft Windows Server 2019		230
Сумарно	-	265,4-477W	5972-24416

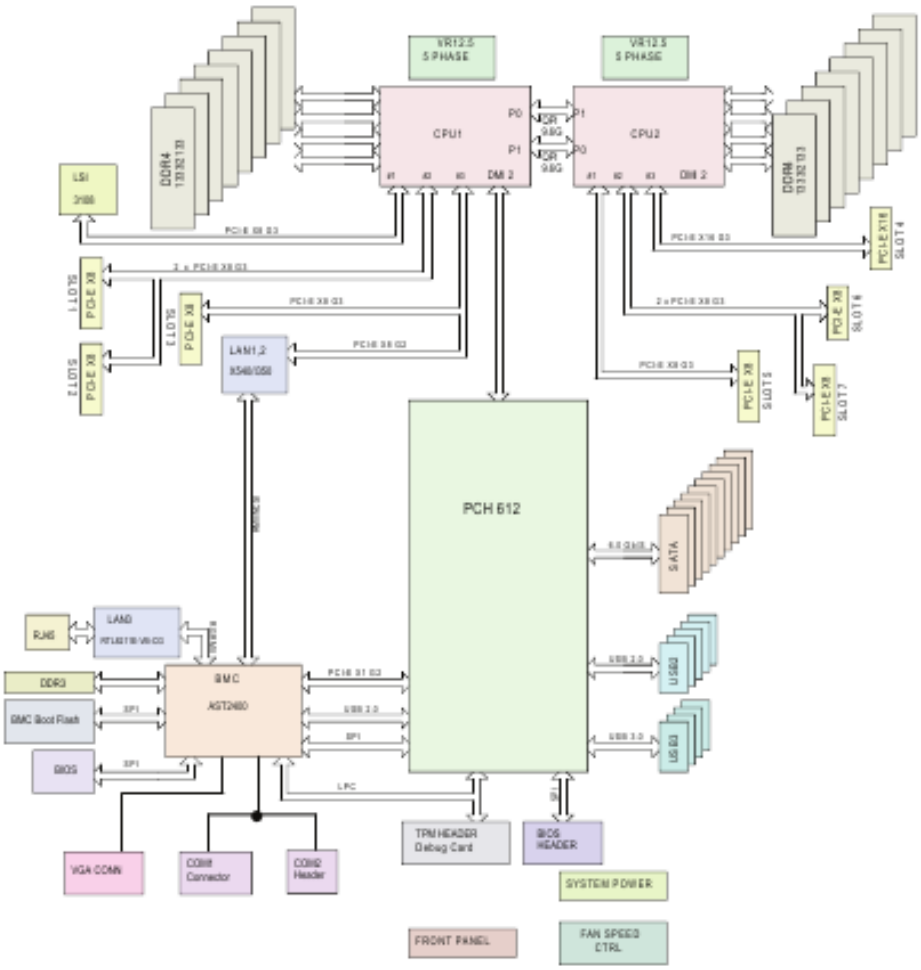


Рис. 2.3 - Структурна схема материнської плати Lenovo ThinkSystem SR650 Server (Xeon SP Gen 2).

На рисунку 2.3 приведена структурна схема материнської плати Lenovo ThinkSystem SR650 Server (Xeon SP Gen 2).

Зовнішній вигляд корпусу Lenovo ThinkSystem SR650 показаний на рисунку 2.4.

Рис.2.4 - Зовнішній вигляд корпусу Lenovo ThinkSystem SR65

ВИСНОВОК ДО РОЗДІЛУ 2

В цьому розділі було зібрано та систематизовану всю необхідну інформацію для створення програмних засобів навчання системних адміністраторів використанню можливостей технологій Intel® vPro™: Trusted Execution-Technology, розроблена серверна платформа Moodle, встановлено необхідне програмне забезпечення для реалізації учбового курсу на розробленій платформі.

РОЗДІЛ 3.
МОЖЛИВОСТІ ТЕХНОЛОГІЇ INTEL TRUSTED EXECUTION TECHNOLOGY

3.1. Що таке технологія Intel® Trusted Execution (Intel® TXT)?

Технологія Intel® Trusted Execution - це набір апаратних розширень для процесорів і чіпсетів Intel®, які покращують платформу Digital Office з такими можливостями безпеки, як вимірюваний запуск і захищене виконання. Технологія Intel Trusted Execution надає апаратні механізми, які допомагають захиститися від програмних атак і захищають конфіденційність і цілісність даних, що зберігаються або створені на клієнтському комп'ютері.

Технологія Intel Trusted Execution надає ці механізми, дозволяючи середовищу, в якому додатки можуть працювати в межах свого власного простору, бути захищеному від усіх інших програмних продуктів в системі. Ці можливості надають механізми захисту, вкорінені в обладнанні, необхідні для забезпечення довіри в середовищі виконання програми. У свою чергу, ці механізми можуть захистити важливі дані і процеси від злому шкідливим програмним забезпеченням, що працює на платформі.

Основна мета платформи Intel® TXT - забезпечити вимірювання запущеного середовища виконання.

Одне вимірювання проводиться, коли платформа завантажується, використовуючи методи, визначені Trusted Computing Group (TCG). TCG визначає корінь довіри для вимірювання (RTM), який виконується на кожному скиді платформи; це створює ланцюжок довіри від скидання до вимірюваного середовища. Оскільки вимірювання завжди виконується при скиданні платформи, TCG визначає цей тип RTM як статичну RTM (SRTM).

Підтримка ланцюга довіри протягом тривалого часу може бути складним завданням тому, що MLE може працювати в середовищі, яке постійно піддається впливу невідомих програмних об'єктів. Щоб вирішити цю проблему, розширена платформа надає інший RTM з інструкціями Intel® TXT. Термінологія TCG для цієї опції - це динамічний корінь довіри для вимірювання (DRTM). Перевага DRTM (його також називають опцією "пізнього запуску") полягає в тому, що запуск вимірюваного середовища може відбутися в будь-який час, не вдаючись до скидання платформи. Можна запустити MLE, виконувати додаток деякий час, припинити MLE, виконувати додаток без віртуалізації, а потім знову запустити MLE. В обох випадках платформа вимірює кожен MLE та забезпечує належне зберігання значення вимірювання MLE.

3.2. Як працює Intel TXT ?

Intel TXT працює над створенням вимірюваного середовища запуску (MLE), що дозволяє точно порівняти всі критичні елементи середовища запуску з "знайомим" джерелом. Intel TXT створює криптографічно унікальний ідентифікатор для кожного затвердженого компонента з підтримкою запуску, а потім надає апаратні механізми примусового контролю для блокування запуску коду, який не відповідає затвердженому коду. Це апаратне рішення забезпечує основу, на якій можна будувати надійні рішення платформ для захисту від програмних атак, що загрожують цілісності, конфіденційності, надійності та доступності систем. Такі успішні атаки створюють дорогі витрати на простої та виправлення, а також потенційно великі витрати, пов'язані з порушенням даних.

Intel TXT забезпечує:

• Перевірений запуск. Апаратний ланцюжок довіри, що дозволяє запустити MLE у "Відомий добрий" стан. Зміни в MLE можна виявити за

допомогою криптографічних вимірювань (на основі хешу чи цифрового підпису).

• Політика управління запуском (LCP). Двигун політики для створення та впровадження виконавчих списків затвердженого виконуваного коду.

• Таємний захист. Апаратурні методи, що видаляють залишкові дані при неправильному відключенні MLE, захищаючи дані від програмного забезпечення, що відслідковує пам'ять та атаки скидання.

• Атестація. Можливість надання даних про вимірювання платформи місцевим, або віддаленим користувачам, або системам для завершення процесу перевірки довіри та підтримки дотримання та аудиту.

3.3. Intel TXT від клієнта до сервера

Спочатку Intel TXT було впроваджено, починаючи з 2007 року в клієнтські платформи на базі технології Intel® vPro ™. Пізніше Intel TXT також поширився на мобільні та серверні платформи. З появою хмарних обчислень та консолідованих віртуалізованих центрів обробки даних потенційна шкода від однієї успішної атаки різко зросла, особливо на кращих мережевих серверах, таких як веб-сервери, портали та менші бази даних.

Intel TXT на серверах, побудованих на основі процесорів Intel® Xeon® Gen 2 Bronze, Silver, Gold, або Platinum, була запущена в 2020 році. Для серверних середовищ (особливо середовищ віртуального сервера), Intel TXT допомагає IT-менеджерам забезпечувати більш високий рівень безпеки системи та конфіденційності інформації в архітектурах корпоративних обчислень. За допомогою апаратних технологій, таких як Intel TXT - та інші технології безпеки Intel, вбудованих у серверні платформи - Intel встановлює галузевий орієнтир для безпечної обробки в центрах обробки даних. Ці будівельні блоки сприятимуть кращому дотриманню регуляторних норм та

підвищуватимуть безпеку та доступність інфраструктури шляхом подолання постійно зростаючих загроз безпеці фізичної та віртуальної інфраструктур.

3.4. Корінь довіри: Фундація безпечніших обчислень

Штрафи за втрачені дані клієнта, працівника або фінансові дані змушують IT-менеджерів не втрачати контроль над своїми системами. Це означає, що вони повинні впроваджувати найкращі інструменти, доступні для захисту своєї інфраструктури та перевірки цілісності обчислювального середовища на постійній основі. Встановлення кореня довіри є важливим. Кожен сервер повинен мати компонент, який завжди буде вести себе очікуваним чином і містити мінімальний набір функцій, що дозволяють описувати характеристики платформи та її надійності.

Потужність технології Intel® TXT встановлює цей корінь довіри, який забезпечує необхідні основи для успішної оцінки обчислювальної платформи та її захисту.

Корінь довіри також забезпечує надійну та стійку до несанкціонованого становища оцінку цілісності будь-яких інших компонентів, що забезпечує впевненість за допомогою безпечного порівняння з очікуваними вимірюваннями. Дозволяючи такі порівняння під час завантаження та запуску послідовності, IT-менеджери можуть зупинити запуск нерозпізнаного програмного забезпечення та застосувати «знайомі» конфігурації часу запуску.

3.5. Захист центру обробки даних віртуального сервера

Рисунок 3.1 показує як Intel TXT захищає центр обробки даних віртуального сервера.

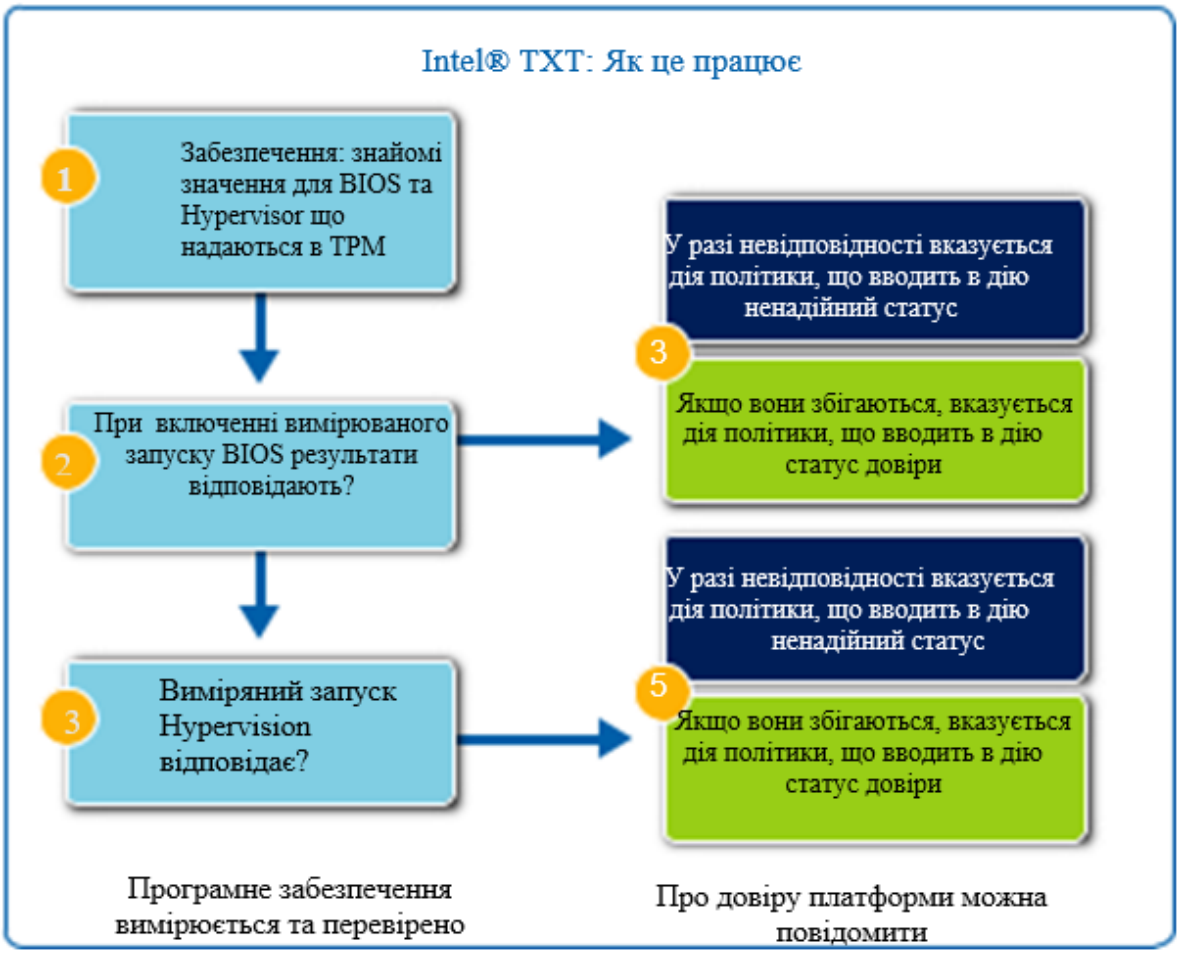


Рис. 3.1 – Технологія Intel® TXT захищає центр обробки даних віртуального сервера

Модель окреслює кроки на високому рівні системи з підтримкою Intel TXT, що оцінює компоненти запуску від раннього BIOS та прошивки системи до гіпервізора. На кожному кроці запуску результатом може бути те, що вимірювання (хеші) компонентів відповідають очікуваним «знайомим» конфігураціям, а запуск дозволений і вказаний як надійний, або що є невідповідність і можна вжити заходів та запуск буде дозволений і вказаний як ненадійний.

У випадку надійного запуску, перевагою є впевненість, що навколишнє середовище було запущено, як очікувалося, без компромісів.

У разі невідповідності можна отримати вказівку на ненадійний запуск. Наприклад, гіпервізор rootkit, такий як "Blue Pill", компрометує систему, намагаючись встановити себе під гіпервізор, щоб ефективно отримати контроль над платформою.

У цьому випадку система з підтримкою Intel TXT має хеш-код, але оскільки він був модифікований (за допомогою вставки руткіта), він не може відповідати "знайомій" конфігурації. У цьому випадку Intel TXT зможе вказати на відсутність довіри і дозволяє вжити заходів. Це демонструє перевагу більшого контролю, який забезпечує Intel TXT над конфігурацією запуску. Це може допомогти зменшити вплив атак зловмисних програм низького рівня.

3.6. Додаткові моделі використання

Забезпечивши контроль, що забезпечує запуск лише надійного гіпервізора на платформі, Intel TXT допомагає захистити сервер перед завантаженням програмного забезпечення для віртуалізації та додає засоби захисту часу запуску, які доповнюють захист від шкідливих програм під час виконання програм, наприклад антивірусне програмне забезпечення та системи виявлення вторгнень. Це цінна модель використання серверу, що дозволяє зменшити витрати на підтримку та відновлення для підприємства.

Хоча цей базовий захист і посилений контроль є ефективним для окремих систем, він стає ще більш потужним, коли враховують сукупні ресурси та динамічні середовища, такі як сьогоднішні віртуалізовані та хмарні реалізації. Ці реалізації, через їхню абстракцію фізичного обладнання та багаторічний рух по спільній інфраструктурі, вимагають більше, ніж традиційних методів, орієнтовані на периметр.

Наприклад, при міграції VM існує реальна стурбованість переміщенням скомпрометованої VM з одного фізичного хоста на інший та потенційною

компрометацією іншого хоста і, можливо, впливає на VM та робочі навантаження на цій платформі. Intel TXT може допомогти боротися з цією проблемою в міграції VM, допомагаючи створити рішення, що відоме як "надійні пули". У цій моделі Intel TXT використовується як основа для створення пулів надійних хостів, в кожному з яких увімкнено Intel TXT і за допомогою якої перевірена цілісність запуску платформи. Потім створюється політика, яка обмежує міграцію віртуальних машин таким чином, що лише ті, хто знаходиться на надійних платформах, можуть бути переміщені на інші довірені платформи. У цьому ж ключі, віртуальним машинам, створених на непідтверджених, або неперевірених платформах, можна запобігти міграції в надійні пули. Це аналогічно пасажиру авіакомпанії, що очищається пунктом пропуску аеропорту, а потім зможе вільно переміщуватися між воротами. Рисунок 3.1 показує, як міграцію VM можна контролювати через ресурси, використовуючи довіру як інструмент управління для міграційної політики. Це дає можливість IT-менеджерам обмежувати конфіденційні дані, або чутливі робочі навантаження платформами, які при цьому краще контролюються за допомогою платформ, що підтримують Intel TXT. Здатність обмежувати міграцію VM лише довіреними хостами продемонстрували Intel, VMware та HyTrust. Ця нова концепція віртуалізованих середовищ викликає великий інтерес у підприємств та клієнтів хмарних постачальників, які шукають нових інструментів розуміння та контролю для віртуальних та хмарних систем. Якщо це має бути значущим контрольним пунктом, менеджерам інформаційних технологій та безпеки потрібен загальний спосіб моніторингу та звітування про події, пов’язані з довірою в їхній інфраструктурі. Ця здатність лежить в основі вирішення проблем із видимістю та дотриманням вимог, посилених віртуалізацією та хмарними архітектурами.

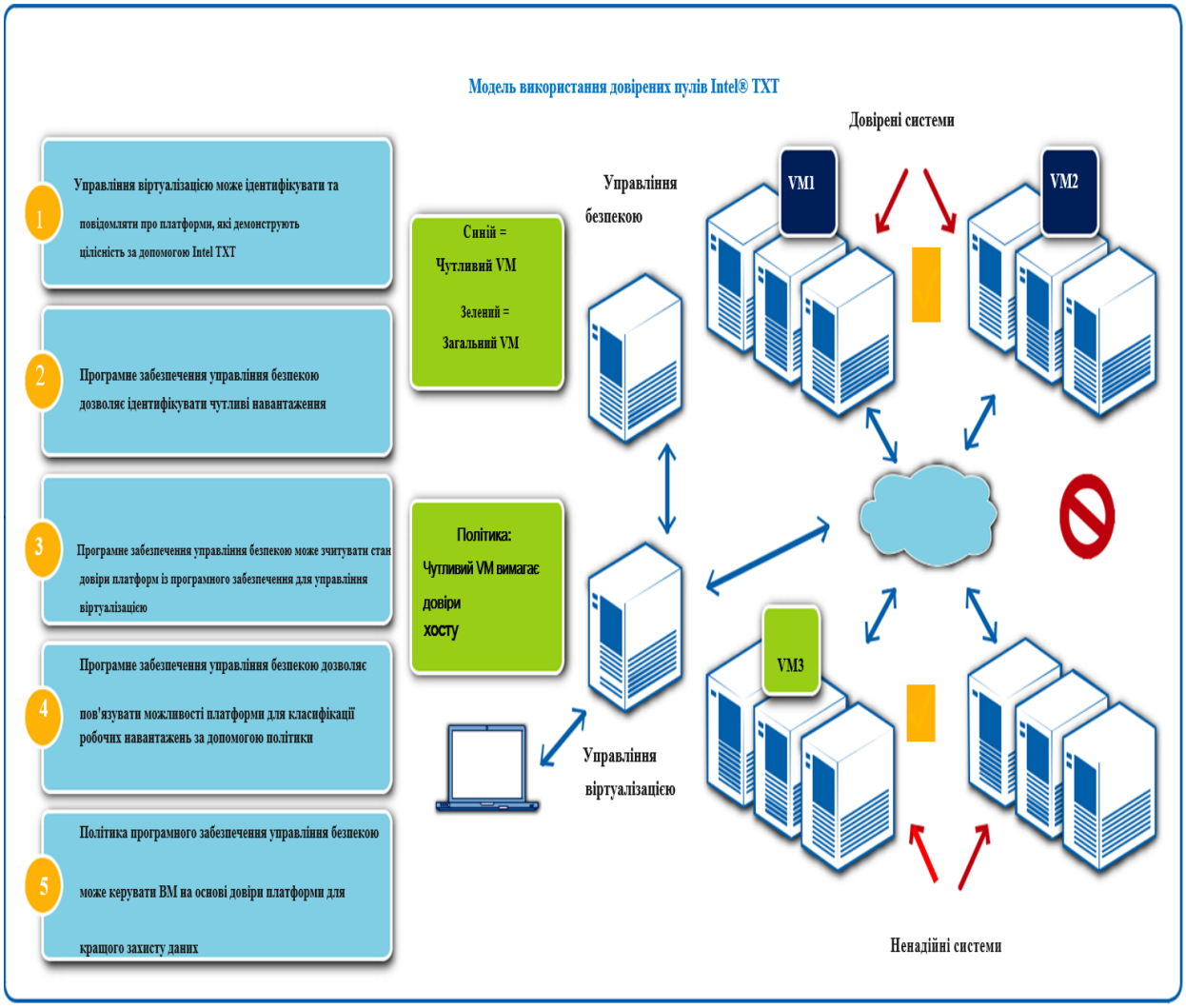


Рис. 3.2 - Надійні пули, створені за допомогою платформи Intel® Trusted Execution Technology (Intel® TXT)

В оперативному режимі це вимагає, щоб статус довіри можна було забезпечити за допомогою консолей управління віртуалізацією та доставити в системи управління інформацією про безпеку (SIEM) та управління, ризик та відповідність (GRC) для більш автоматизованого ведення журналів, звітності та аудиту.

Звичайно, для всіх моделей використання потрібен повний пакет рішень апаратних та програмних компонентів. Intel тісно співпрацює з провідними ОС, VMM (або гіпервізором) та іншими незалежними постачальниками програмного забезпечення, щоб включити підтримку Intel TXT для забезпечення більш безпечних, більш захищених серверних платформ та

рішень центрів обробки даних через ці та інші інноваційні моделі використання.

3.7. Компоненти Intel TXT

Серверні платформи Intel® з Intel TXT включають кілька нових нововведень безпечної обробки. Як показано на рисунку 3.3, вони включають:

• Довірені розширення, інтегровані в кремній (процесор Intel Xeon і чіпсет Intel®)

• Аутентифіковані модулі коду (ACM)

• Інструменти LCP

Не всі компоненти, необхідні для платформи Intel TXT, надходять безпосередньо від Intel. Важливі компоненти також надходять від сторонніх осіб, включаючи:

• Модуль надійної платформи (TPM) 2.0;

• BIOS з підтримкою Intel TXT;

• Середовище гіпервізора чи ОС.

Платформа повинна включати всі ці компоненти для включення Intel TXT. Якщо один з цих компонентів відсутній або несправний, платформа перейде в традиційний, ненадійний стан. Зауважте, що Intel TXT також широко використовує технологію віртуалізації Intel® (Intel® VT) при використанні у віртуалізованому середовищі, щоб забезпечити захист від несанкціонованого прямого доступу до пам'яті (DMA), а також для забезпечення застосувань та ізоляції даних у системі.

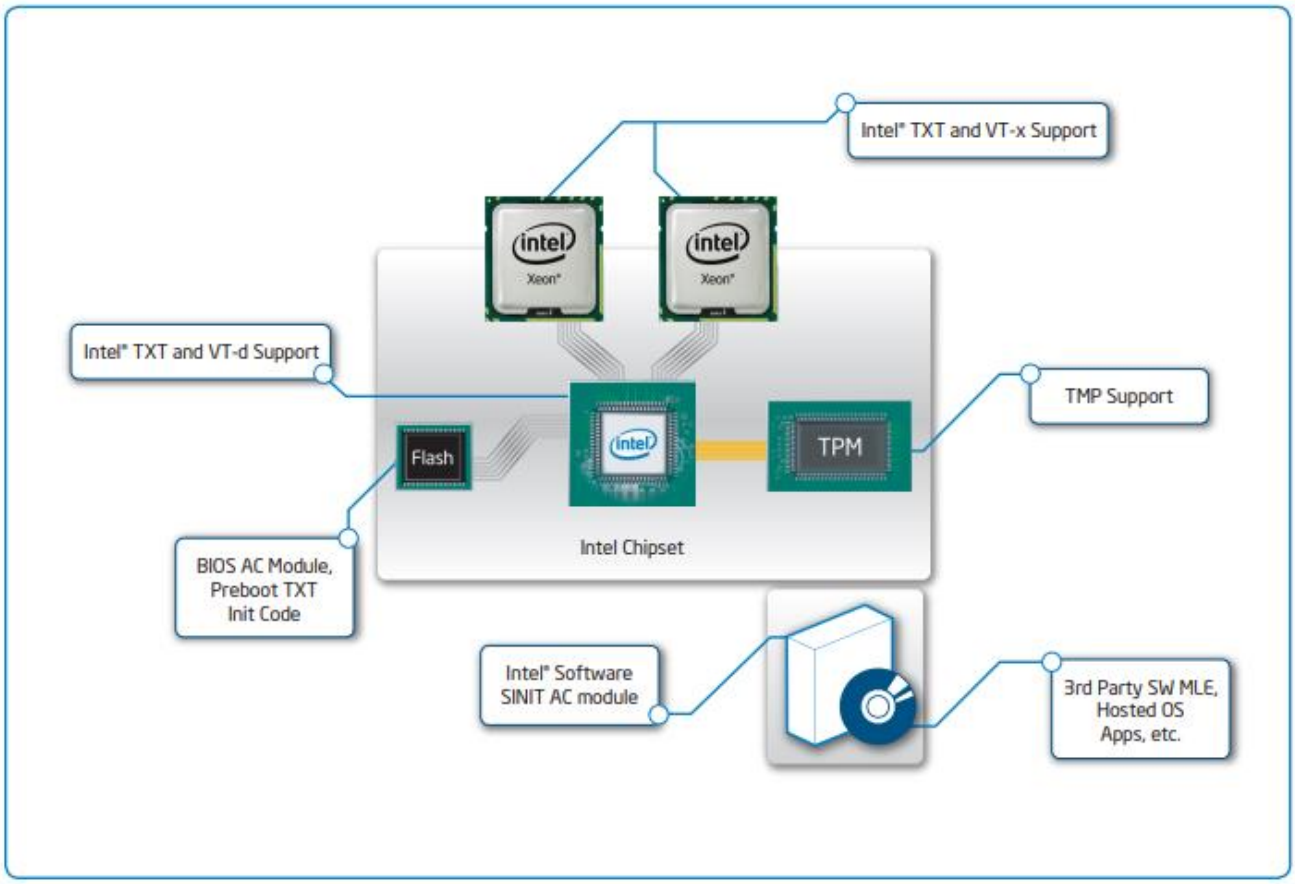


Рис. 3.3 – Компоненти Intel TXT **[4]**

3.8. Використання TPM

Intel® TXT широко використовує модуль надійної платформи (TPM), визначений Trusted Computing Group (TCG) у "Основній специфікації TPM для сім'ї TPM 1.2" та "Специфікація бібліотеки TPM для сім'ї TPM 2.0". TPM забезпечує сховище для вимірювань та механізми використання вимірювань. Система використовує вимірювання як для повідомлення про поточну конфігурацію платформи, так і для забезпечення довгострокового захисту конфіденційної інформації.

TPM зберігає вимірювання в регістрах конфігурації платформи (PCR). Кожна PCR забезпечує зону зберігання, яка дозволяє необмежену кількість вимірювань у фіксованому обсязі простору. Вони забезпечують цю особливість притаманною властивістю криптографічних хешів.

Зовнішні суб'єкти ніколи не записують безпосередньо в регістр PCR, вони "розширюють" вміст PCR. Операція розширення приймає поточне значення PCR, додає нове значення, виконує криптографічний хеш на комбінованому значенні, а хеш-результат - нове значення PCR. Однією з властивостей криптографічних хешів є те, що вони залежать від порядку. Це означає, що хешування A та B дає результат, що відрізняється від хешування B та A. Ця властивість впорядкування дозволяє вмісту PCR вказувати порядок вимірювань.

Відправлення вимірювальних значень від вимірювального агента до TPM є критичним завданням платформи. Динамічний корінь довіри для вимірювання (DRTM) вимагає, щоб конкретні повідомлення надходили з DRTM до TPM. Intel® TXT DRTM - це інструкція GETSEC [SENTER]. Система забезпечує GETSEC [SENTER] спеціальними повідомленнями для зв'язку з TPM.

Крім вимірювань, Intel® TXT використовує енергонезалежну (NV) оперативну пам'ять TPM для зберігання даних політики управління запуском (LCP) та для зв'язку між ACM. Три основні індекси, що використовуються Intel® TXT, позначаються як AUX (допоміжний), PO (власник платформи) та Intel® Software Guard Extension (Intel® SGX) (розширення програмного забезпечення). Детально інформація про ці індекси буде представлено нижче. З випуском специфікації TPM 2.0 та підтримуючих пристроїв для запуску Intel® TXT може знадобитися багато змін. Пристрої TPM 2.0 можуть підтримувати різні криптографічні алгоритми, а один пристрій часто підтримуватиме кілька дайджестів і асиметричні алгоритми підпису. MLE та ACM визначають сімейство платформ TPM.

3.9. Політика управління запуском

Політика управління запуском (LCP) - це механізм підтвердження для перевіреного процесом запуску Intel® TXT. LCP використовується для визначення, чи відповідає поточна конфігурація платформи або середовище, яке потрібно запустити, заданим критеріям. Політика може визначатися власником платформи, а також використовуватися під час перевірки завантаження (BtG).

LCP дозволяє власнику платформи (PO) задавати середовища, які можуть бути запущені інструкцією GETSEC [SENTER].

Додавання LCP до платформи опосередковано тепер робить їх більш керованими.

Замірені середовища, що запускаються (MLEs), більше не повинні турбуватися про прикріплення секретів до декількох конфігурацій платформи, коли вони знають, що існує політика, щоб перевірити їх до їх запуску; їм просто потрібно прикріпити представництво цієї політики. Це стає корисним, коли змінюється конфігурація платформи, наприклад BIOS замінюється, оскільки нові конфігурації BIOS можуть бути додані до політики, що не потребує змінення будь-якого секрету MLE - таким чином зменшується тягар міграції секретів MLE, якщо змінюється інший компонент платформи. Вимоги LCP можна визначити як:

- Надати власнику платформи можливість контролювати, які вимірювані середовища можуть бути негайно запущені інструкцією GETSEC [SENTER].
- Надати власнику платформи можливість контролювати, які конфігурації платформи, виміряні статичним коренем довіри, дозволяють виконувати GETSEC [SENTER].

- Надати власнику платформи можливість контролювати, яким STM дозволено запускати постачальників SMRAM та MLE, щоб вони могли вимагати присутності STM.
- Забезпечте цей механізм таким чином, щоб він не підривав ненадійне програмне забезпечення.
- Якщо на платформі немає жодної політики, платформа повинна продовжувати процес запуску Intel® TXT, дозволяючи запускати будь-яку конфігурацію та MLE.

3.10. Індекс Auxiliary

Нижче наведені основні властивості допоміжного індексу режиму TPM 1.2 (AUX):

Він визначається набором бітів "D", що означає, що індекс визначено протягом життя, а платформа не може бути видалена.

Вміст індексу читається будь-яким SW в будь-якій локації, але він може бути записаний лише через TPM, тобто лише ACM.

Індекс AUX режиму TPM 2.0 має властивості, аналогічні його режиму TPM 1.2, але також має помітні відмінності:

Як і індекс режиму TPM 1.2, його вміст читається будь-яким ПЗ та доступний для запису лише через ACM.

Її розмір більший для розміщення більш великих дайджестів, вироблених SHA256 та SHA384 алгоритмами.

Найбільша відмінність від його аналога TPM 1.2 - це можливість видалити цей індекс відповідно до політики постачальника платформи.

Ще одна важлива відмінність пов’язана з індексом nameAlg - одним з основних, що визначають міцність захисту даних.

3.11. Індекс власника платформи

Метою індексу власника платформи (PO) є розміщення політики LCP власника платформи.

Незважаючи на те, що властивості TPM 1.2 та TPM 2.0 дуже схожі, все ж помітні відмінності існують:

У режимі TPM 1.2 індекс PO контролюється даними власника платформи. Його можна прочитати будь-яким SW, але може бути записаний / видалений лише власником платформи. Усі читання та записи можливі в будь-якій локації.

У режимі TPM 2.0 індекс PO контролюється обліковими даними власника платформи. Це також може бути прочитаний будь-яким SW та записаний / видалений лише власником платформи.

Розмір індексу може змінюватись (але також може бути встановлений за максимальним значенням), залежно від розмірів дайджеста, що зберігаються в області PolicyHash.

Як і індекс AUX режиму TPM 2.0, він вимагає ретельного вибору nameAlg.

3.12. Intel® SGX вимоги до Intel® TXT платформи

Розширення програмного забезпечення Intel® Software Guard (Intel® SGX) - це набір інструкцій та механізмів доступу до: пам'яті, доданих, процесорів з Intel® Architecture. Ці розширення дозволяють додатку створювати захищений контейнер, який називається анклавом. Анклав - це захищена зона в адресному просторі програми, яка забезпечує конфіденційність та цілісність навіть за наявності привілейованих шкідливих програм. Доступ до області пам'яті анклаву від будь-якого програмного забезпечення, яке не знаходиться в анклаві, запобігається.

Оскільки ACM-модулі Intel® TXT знаходяться в довіреній обчислювальній базі (TCB) Intel® SGX, Intel® SGX SW повинен бути обізнаний про номери версій безпеки Intel® SGX (Intel® SGX SVN) всіх ОСБ в системі. Передача ACM Intel® SGX SVN до Intel® SGX SW здійснюється за допомогою спеціалізованого програмування BIOS_SE_SVN MSR, за яке відповідає BIOS. Це завдання BIOS є тривіальним, якщо всі ОСБ в системі переносяться у флеш-пам'яті BIOS, але представляє особливий виклик клієнтським платформам, що переносять SINIT ACM на жорсткий диск, де він не доступний для вивчення BIOS.

З метою уникнення негідних скидів результатів невідповідності очікуваного та фактичного SVN (номер версії безпеки) SINIT ACM під час запуску Intel® SGX та Intel® TXT, вимоги Intel® SGX, Intel® TXT та інтерфейсу BIOS, розроблені для клієнта платформи повинні дотримуватися.

Інтерфейс дозволяє програмному забезпеченню Intel® TXT передати BIOS значення SINIT SVN, яке буде використано під час наступного POST. У гіршому випадку потрібне ще одне перезавантаження системи після оновлення SINIT в стеку програмного забезпечення Intel® TXT.

Інтерфейс базується на механізмі поштової скриньки, реалізованому як Intel® SGX TPM NV індекс з необмеженими можливостями читання і запису. Програмне забезпечення для виконання програми Intel® TXT запише в цей індекс, коли Intel® SGX SVN виявиться в SINIT ACM і BIOS прочитає цей індекс та запрограмує поле SINIT_SVN BIOS_SE_SVN MSR. **[5]**

3.13. Встановлення кореня довіри з Intel TXT для серверів

Існує два чіткі методи встановлення довіри до обчислювального середовища. Перший метод називається статичним коренем довіри для вимірювання (S-RTM). У моделях S-RTM вимірювання починається з події скидання платформи та непорушного кореня (наприклад, завантажувальний

блок BIOS) і продовжується в ОС та її компонентах. Основна перевага S-RTM - це його простота. Його недолік полягає в тому, що лише S-RTM у складній системі може призвести до великої та некерованої бази довірених обчислень (TCB) - набору компонентів, необхідних для визначення платформи, як довіреною. Якщо будь-який з компонентів процесу завантаження / запуску зміниться (або оновиться) після встановлення довіри, система вимагає міграції або повторного запечатування секретів.

Інший метод встановлення довіри до обчислювального середовища - це динамічний корінь довіри для вимірювання (D-RTM). D-RTM зазвичай призводить до меншої кількості TCB - що бажано. У D-RTM довірчі властивості компонентів можна ігнорувати доти захищена подія (наприклад, включений запуск гіпервізора) запускає та ініціює систему, починаючи з початкового кореню вимірювання. Компоненти, що ставились перед подією захисту D-RTM, будуть виключені з TCB і не можуть бути виконані після встановлення довірчих властивостей системи.

Intel розробила архітектуру Intel TXT для серверів, оскільки серверне середовище представляє складні сценарії завантаження. Тому в TCB сервера важливо ввести в деякі частини раннього BIOS, які ініціюють системне середовище та компоненти BIOS під час виконання (також називаються кодом управління системою). Вони необхідні для реалізації функцій надійності, доступності та зручності обслуговування (RAS) сервера. Отже, оскільки чиста реалізація D-RTM виключає ці пункти, справжня реалізація D-RTM з меншою TCB стає недостатньою.

Щоб створити більш підходящу реалізацію для серверів, Intel TXT використовує основні функції обох підходів. У будь-якій комп'ютерній системі певні компоненти (як апаратні, так і програмні) повинні знаходитись у межах довіри TCB, щоб виявити стан запуску. У довірчій моделі Intel TXT

частина програмного забезпечення для завантаження системи дозволена в межах довіри захищеного обладнанням середовища.

Насправді Intel TXT дозволяє отримати достатню кількість системного програмного забезпечення в межах довіри, щоб можна було підтримувати всі поточні або прогнозовані функції RAS. Крім того, архітектура Intel TXT запозичує модель S-RTM, надаючи методи для вимірювання та запису в TPM будь-яку із системних програмних програм, що знаходяться в межах довіри - надаючи додаткову можливість виявлення атак на цей чутливий компонент платформи.

В архітектурі Intel TXT надійні вбудовані програмні засоби найчастіше включатимуть компоненти BIOS, які ініціюють середовище системи, модулі, які беруть участь у впровадженні функцій системи RAS, що потребують модифікації середовища системи, та будь-якого коду системного процесора.

3.14. Увімкнення Intel TXT

Intel тісно співпрацює з галузевими партнерами, щоб забезпечити безпечніші та надійніші серверні платформи та центри обробки даних. Як зазначалося раніше, рішення з підтримкою Intel TXT вимагають компонентів від багатьох постачальників для забезпечення відповідного захисту платформи. Intel TXT потребує серверної системи з Intel VT, процесору з підтримкою Intel TXT, чіпсету Intel, ACM, BIOS та сумісного MLE (ОС або гіпервізору) з Intel TXT. Крім того, Intel TXT вимагає, щоб система містила TPM, як визначено Trusted Computing Group (http: //www.trustedcomputinggroup. Org) і певного програмного забезпечення для деяких застосувань. А більш просунуті довірені пули та моделі використання, орієнтовані на дотримання вимог, також вимагають механізмів політики безпеки, інструментів управління безпекою та відповідністю.

Intel докладає зусиль для охоплення всіх компонентів, описаних вище, працює з постачальниками, щоб забезпечити вказівки щодо необхідних апаратних компонентів (включаючи сумісні TPM). Це надає засоби LCP та LCP для полегшення тестування та перевірки компонентів Intel TXT.

Аналогічно, Intel працює з постачальниками ОС та гіпервізорів, щоб допомогти їм розробити програмні пакети для Intel TXT.

LCP - компонент, який заслуговує на особливу увагу. Він використовується всіма постачальниками компонентів Intel TXT. Це також інструмент, який IT-менеджери використовуватимуть для контролю над своїм оточенням.

Як двигун політики, LCP працює на структурах даних про політику, які укорінені та захищені компонентом платформи TPM. TPM містить політику, збережену виробником сервера та політику, що зберігається власником. Ці політики визначають, які значення представляють "відомий товар", або бажаний дайджест завантаження програмного забезпечення. Правила двигуна політики диктують, що встановлена політика власника платформи замінює політику збереженого набору. Це дозволяє виробнику сервера вказувати на MLE, встановлений на заводі та в той же час надає можливість власнику платформи (наприклад, IT-менеджеру) оновити або замінити її на власний вибір MLE.

Постачальники систем та програмного забезпечення будуть індивідуально розкривати підтримку Intel TXT для своїх конкретних продуктів, Intel також надає на своєму веб-сайті вичерпний перелік платформ, програмних продуктів та постачальників послуг, які оголосили про підтримку Intel TXT. **[4]**

ВИСНОВОК ДО РОЗДІЛУ 3.

Більшість інструментів попередження зловмисних програм виконується лише після завантаження системи в середовище виконання. У епоху постійно зростаючих загроз від атак гіпервізора, атак BIOS, зловмисних кореневих комплектів тощо, Intel TXT допомагає усунути важливий пробіл у безпеці, надаючи оцінку середовищу запуску та примушуючи виконувати "знайомий" код.

Апаратні засоби Intel TXT дозволяють краще контролювати стартовий стек серверних систем та здійснити його ізоляцію в процесі завантаження.

Сьогодні, як ніколи, підприємства та організації потребують такого захисту, щоб забезпечити захист критичних даних клієнтів, працівників та фінансових даних.

Завдяки Intel TXT-рішенням підприємства та організації можуть:

• Вирішувати зростаючі загрози безпеці у вашій фізичній та віртуальній інфраструктурі;

• Сприяти дотриманню урядових та галузевих норм та стандартів захисту даних;

• Скоротити витрати на підтримку та відновлення програм, пов’язаних із зловмисним програмним забезпеченням;

• Встановити видимість цілісності фізичної та віртуальної інфраструктури.

РОЗДІЛ 4
МОЖЛИВОСТІ TPM

4.1. Модуль надійної платформи (TPM)

Intel TXT широко використовує модуль довіреної платформи (TPM), компонента, визначеного Trusted Computing Group (TCG). TPM надає низку функцій захисту. Зокрема, TPM забезпечує надійне сховище для вимірювань та механізми використання цих вимірювань. Система використовує вимірювання як для звітування, так і для оцінки поточної конфігурації платформи та для забезпечення довгострокового захисту конфіденційної інформації.

Платформа BIOS спеціально розроблена для налаштування платформи безпечного режиму роботи. BIOS відіграє значну роль, до складу обов'язків якої входять:

• Постачання ACM. ACM створені постачальником мікросхем і надаються в BIOS розробник, який повинен бути включений до складу образу BIOS.

• Налаштування платформи для роботи Intel TXT.

• Проведення перевірки безпеки та реєстрація в ACM.

• Блокування конфігурації платформи за допомогою інструкції щодо безпеки процесора GETSEC.

Після блокування BIOS інша прошивка більше не може змінювати конфігурацію. BIOS виконує це блокування раніше виконання будь-якого стороннього коду.

4.2. Роль TPM

Важко говорити про Intel TXT, не звертаючись до TPM. TPM є важливим компонентом для покращення безпеки.

В даний час платформи містять TPM, які відповідають версії 2.0. Вона забезпечує ту ж функціональність, що і TPM версії 1.2 плюс включає в себе розширені можливості та потужності. Основні функції безпеки, що надаються TPM версії 1.2, проілюстровано на рис. 4.1.

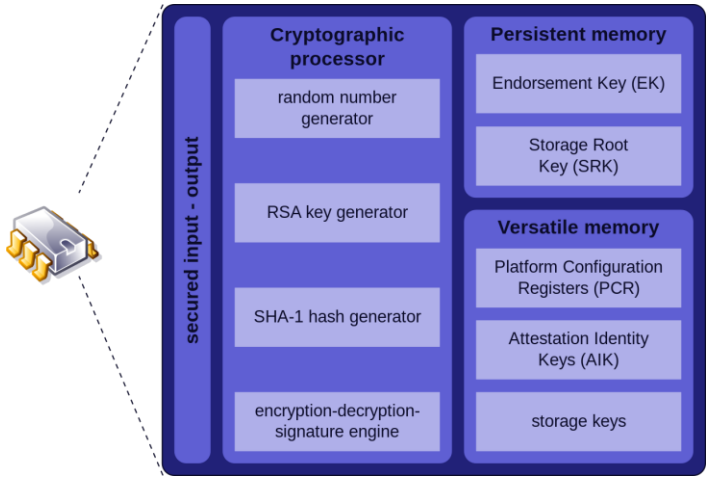


Рис. 4.1 – Основні функції безпеки модулю ТПМ версії 1.2

4.3. Інтерфейс TPM

Інтерфейс TPM простий, що спрощує захист. TPM підключається до чипсету за допомогою шини Low Pin Count (LPC) і доступ до нього здійснюється лише через регістри вбудованого вводу-виводу (MMIO), захищені чипсетом. Це означає, що пристрої вводу / виводу взагалі не можуть отримати доступ до TPM і ОС може легко контролювати, які процеси мають доступ до TPM. Крім того, TPM застосовує додаткові захисти та права доступу.

4.4. Конфіденційні рівні

TPM має різні конфіденційні рівні. Елемент кожного рівня має доступ до іншого рівня, що дозволяє контролювати доступ до кожного рівня як апаратним, так і програмним засобам. Набір чіпів визначає, які локальні пункти активні (тобто чи буде ігноруватися читання чи запис на цьому рівні), а системне програмне забезпечення може контролювати, які процеси мають доступ до цих сторінок за допомогою звичайного управління пам’яттю та пейджинговими функціями. Є п'ять конфіденційних рівнів (від 0 до 4), які Intel TXT використовує так, як показано на (рис. 4.2)

Locality	Access
0	Always open for general use.
1	Operating system (not used as part of TXT).
2	System software (OS) in secure mode. Only after the OS has successfully performed a secure launch. The OS may close this access at any time.
3	ACMs. Only an ACM that has been invoked by the GETSEC instruction has access to locality 3.
4	Hardware. Only the processor executing its microcode has Locality 4 access.

Рис. 4.2 – Конфіденційні рівні TPM **[6]**

4.5. Практичне застосування

На комп'ютерах з TPM можна встановлювати і створювати сертифікати. Після налаштування комп'ютера, закритий ключ RSA для сертифіката прив'язується до TPM і не може бути експортований. TPM також можна використовувати в якості заміни смарт-карток, що скорочує витрати часу, пов'язані зі створенням додатків по оплаті смарт-карткою.

Автоматизована підготовка в TPM знижує вартість розгортання TPM на підприємстві. Нові API для керування TPM можуть визначити, чи потрібне для підготовки TPM фізична присутність фахівця для підтвердження запитів на зміну стану TPM під час завантаження.

Антишкідливе ПО може використовувати виміряні показники завантаження операційної системи, щоб підтвердити цілісність комп'ютера з операційною системою Windows 10, або Windows Server 2019. При цьому запускається Hyper-V, щоб переконатися, що центри обробки даних, використовують віртуалізацію, котра не запускає недовірених низькорівневих оболонок. Разом з мережевою розблокуванням BitLocker IT-адміністратори можуть передавати оновлення, при цьому комп'ютер не чекатиме введення ПІН-коду.

У TPM є ряд параметрів групової політики, які можна використовувати для управління його використанням. Їх можна застосовувати для управління значенням авторизації власника, для блокуванням звичайних користувачів і архівації даних TPM.

4.6. Атестація працездатності пристрою

Атестація працездатності пристрою дозволяє підприємствам встановити відношення довіри на основі апаратних і програмних компонентів керованого пристрою. За допомогою атестації працездатності пристрою можна налаштувати MDM-сервер для запиту служби підтвердження працездатності, що дозволить або заборонить доступ до безпечного ресурсу з боку керованого пристрою.

За допомогою пристрою можна перевірити наступне:

- Запобігання виконання даних підтримується і включено?
- Шифрування диска BitLocker підтримується і включено?
- Безпечне завантаження підтримується і включена? **[7]**

4.7. Зовнішній модуль TPM

Розглянемо приклад використання зовнішнього TPM модуля. На платі встановлений спеціальний роз'єм, окремо поставляється сам TPM модуль, що

розміщується на власній платі (див. рис. 4.3 та рис. 4.4). Однак зазвичай TPM модуль розпаюється безпосередньо на материнській платі.

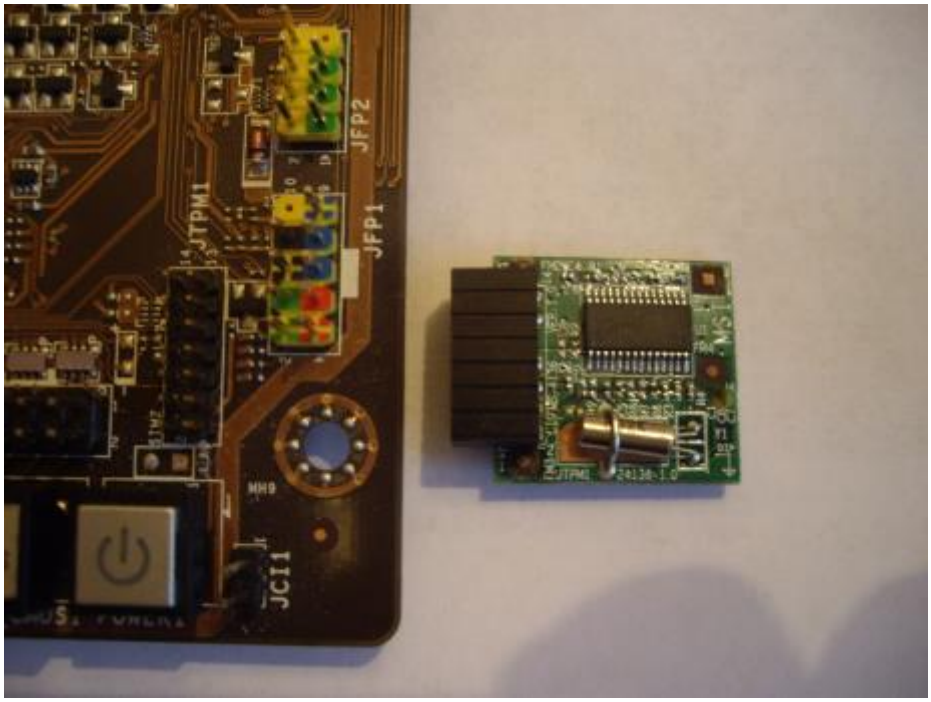


Рис. 4.3 - TPM модуль і роз'єм для його підключення на материнській платі

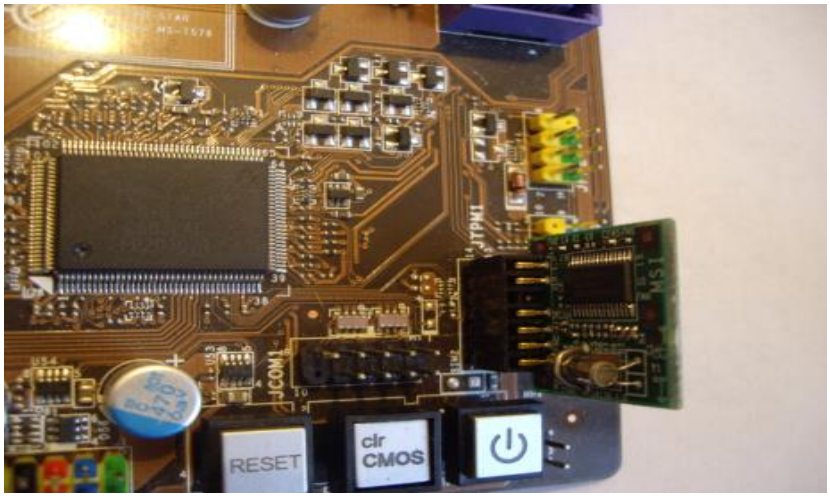


Рис. 4.4 – Підключення зовнішнього TPM модулю

Передбачалося, що для запуску гіпервізора буде використовуватися спеціальний довірений режим, в якому стартовий код системи віртуалізації буде запускатися тільки після перевірки його на цифровий підпис в TPM модулі в спеціальному апаратному циклі (для виключення можливості

програмної емуляції). Крім цього стан апаратури процесора в момент запуску гіпервізора буде однозначно виключати можливість роботи в емуляційному середовищі і в режимі трасування / крокового налагодження.

Фірма AMD для цього ввела спеціальну команду SkInit в систему віртуалізації, і стала називати свою технологію віртуалізації SVM - секретна віртуальна машина.

Фірма INTEL порахувала, що однієї команди мало і ввела новий режим роботи процесора, - Safer Mode Extensions (SMX). Для цього розширення була введена одна багатофункціональна команда GetSec, в залежності від параметра вона виконує вхід / вихід в спеціальний режим логічного довіреного процесора.

Специфікаціям TPM і самих модулів більше десяти років, дані пристрої замислювалися в той час, коли про апаратуру віртуалізації навіть не мріяли, тому зараз ця технологія хоч і застосовується, але легко контролюється засобами віртуалізації, чому як приклад демонструє версія гіпердрайвера - «Червона пігулка».

За допомогою гіпердрайвера можна контролювати протоколи роботи різних пристроїв, причому контролювати навіть пристрої, призначені для захисту обчислювальних систем, що мають спеціальні системи захисту від нелегального втручання, - не тільки TPM модулі, а й різні смарт-карти, всілякі токени.

Демонстраційна версія гіпердрайвера «Червона пігулка» в варіанті контролю пристроїв модифікована і на платформу віртуалізації навішені специфічні обробники, контролюючі адресні простори TPM модуля, при спробах будь-яких програмних засобів звернутися до даних апаратних ресурсів, гіпердрайвер реєструє ці події в дампі, дамп можна переглянути через Гіперагента.

Крім реєстрації апаратної події реєструється адреса команди в програмному модулі, що виконує дане звернення до апаратури. Гіперагент

дозволяє переглянути ці програмні модулі і при необхідності зберегти їх у файлі для подальшого аналізу.

Найпоширенішим програмним засобом, що використовують TPM модуль для зберігання ключів шифрування є Bitlocker саме за роботою цієї програми і спостерігає гіпердрайер «Червона пігулка» на наведеному нижче рис. 4.5

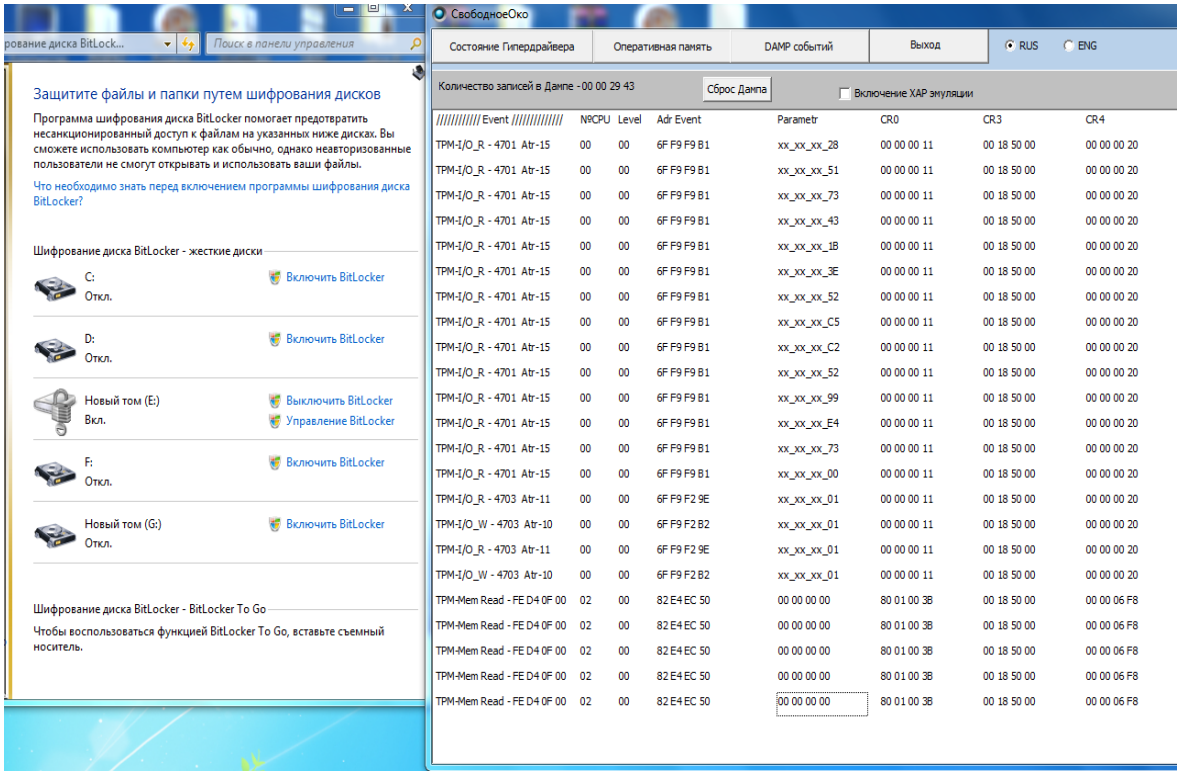


Рис. 4.5 - Протокол роботи Бітлокера з TPM модулем

Спеціальною службою Windows також контролюється адміністрування TPM модуля, наприклад, зареєстрований протокол ініціалізації чистого TPM модуля і введення в нього ключа активації. **[8]**

4.8. BitLocker

Шифрування диска BitLocker - це функція захисту даних, яка інтегрується в операційну систему і запобігає загрози розкрадання даних або розкриття інформації на втрачених, вкрадених або неправильно виведених з експлуатації комп'ютерах.

BitLocker забезпечує максимальний захист при використанні з довіреною платформним модулем (TPM) версії 1.2 або вище. Довірений платформний модуль - це апаратний компонент, який виробники встановлюють на багатьох нових комп'ютерах. Спільно з BitLocker він забезпечує захист даних користувачів і запобігає несанкціонований доступ до комп'ютера, поки система знаходиться поза мережею.

На комп'ютерах без модуля TPM версії 1.2 або більш пізньої все одно можна зашифрувати диск операційної системи Windows за допомогою BitLocker. Але при такій реалізації користувач повинен вставити USB-накопичувач з ключем запуску, щоб запустити комп'ютер або вивести його зі сплячого режиму.

На додаток до можливостей модуля TPM компонент BitLocker дозволяє блокувати звичайний процес запуску до тих пір, поки користувач не введе ПІН-код або не встановить знімний пристрій (наприклад, USB-накопичувач) з ключем запуску. Ці додаткові заходи безпеки забезпечують багатофакторну перевірку справжності та запобігають запуску комп'ютера або його виведення з режиму глибокого сну, якщо не вказано правильний ПІН-код, або не надано ключ запуску.

Спочатку Бітлокер (на етапі завантаження ОС) користується функціями БІОС для зчитування ключів шифрування дисків з TPM модуля, робота йде через адресний простір портів введення / виводу. Після завантаження ядра ОС операційна система починає сама працювати з модулем по протоколу 1.2 і обмін інформацією здійснюється вже через адресний простір MMIO. **[9]**

4.9. Налагодження TPM модуля в BIOS

Для включення модуля зайдіть в BIOS і перейдіть в розділ, пов'язаний з безпекою. Хоча BIOS може істотно відрізнятися на різних комп'ютерах, як правило, розділ з настройками безпеки називається "Security". У цьому розділі повинна бути опція, яка називається "Security Chip" (див. рис. 4.6).

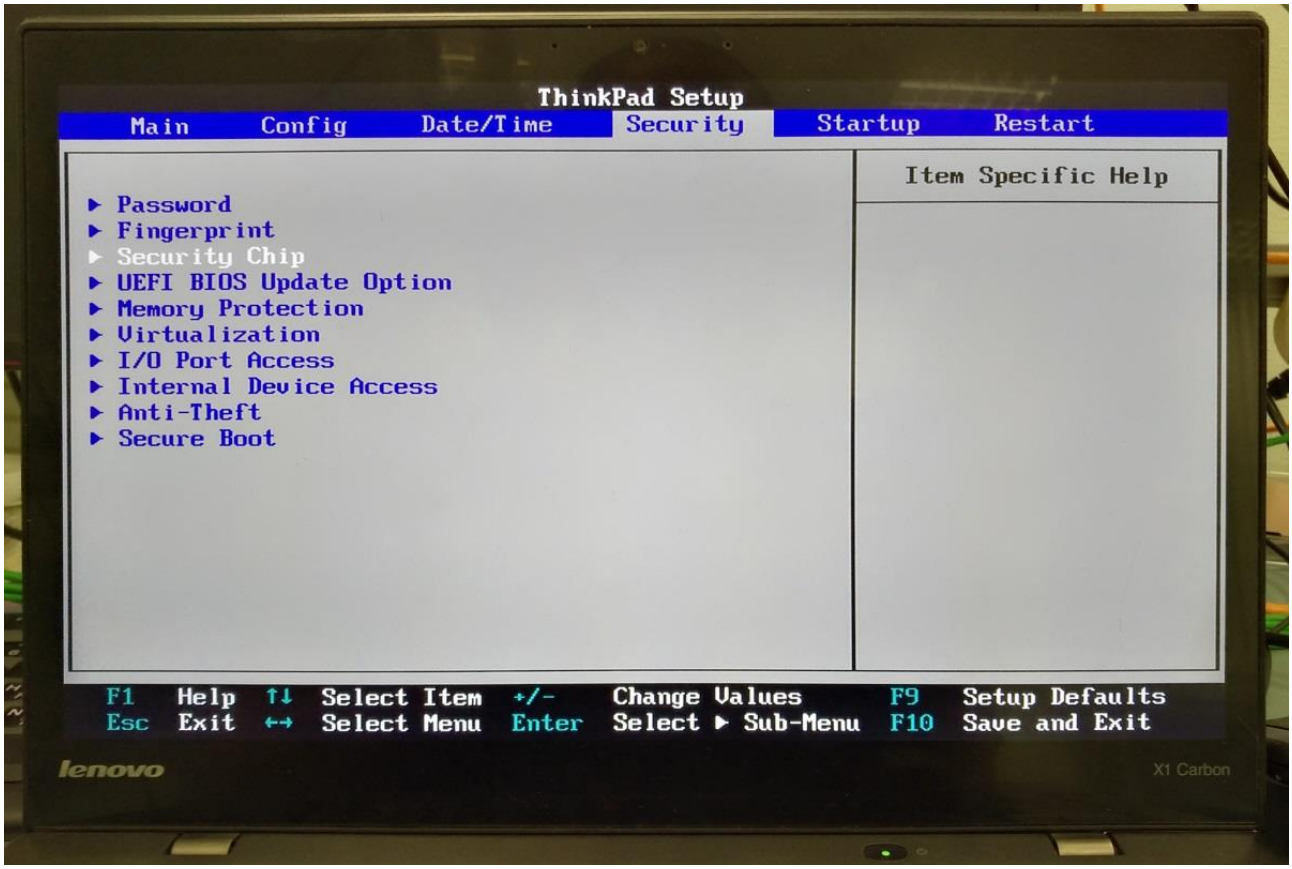


Рис. 4.6 - Налаштування безпеки в BIOS

Модуль може перебувати в трьох станах:

- Вимкнений (Disabled).
- Включений і не задіяний (Inactive).
- Включений і задіяний (Active).

У першому випадку його не буде видно в операційній системі, у другому - він буде видно, але система не буде його використовувати, а в третьому - чіп можна бачити і він буде використовуватися системою.

Тут же в налаштуваннях можна очистити старі ключі, що згенеровані чіпом TPM (див. рис. 4.7).

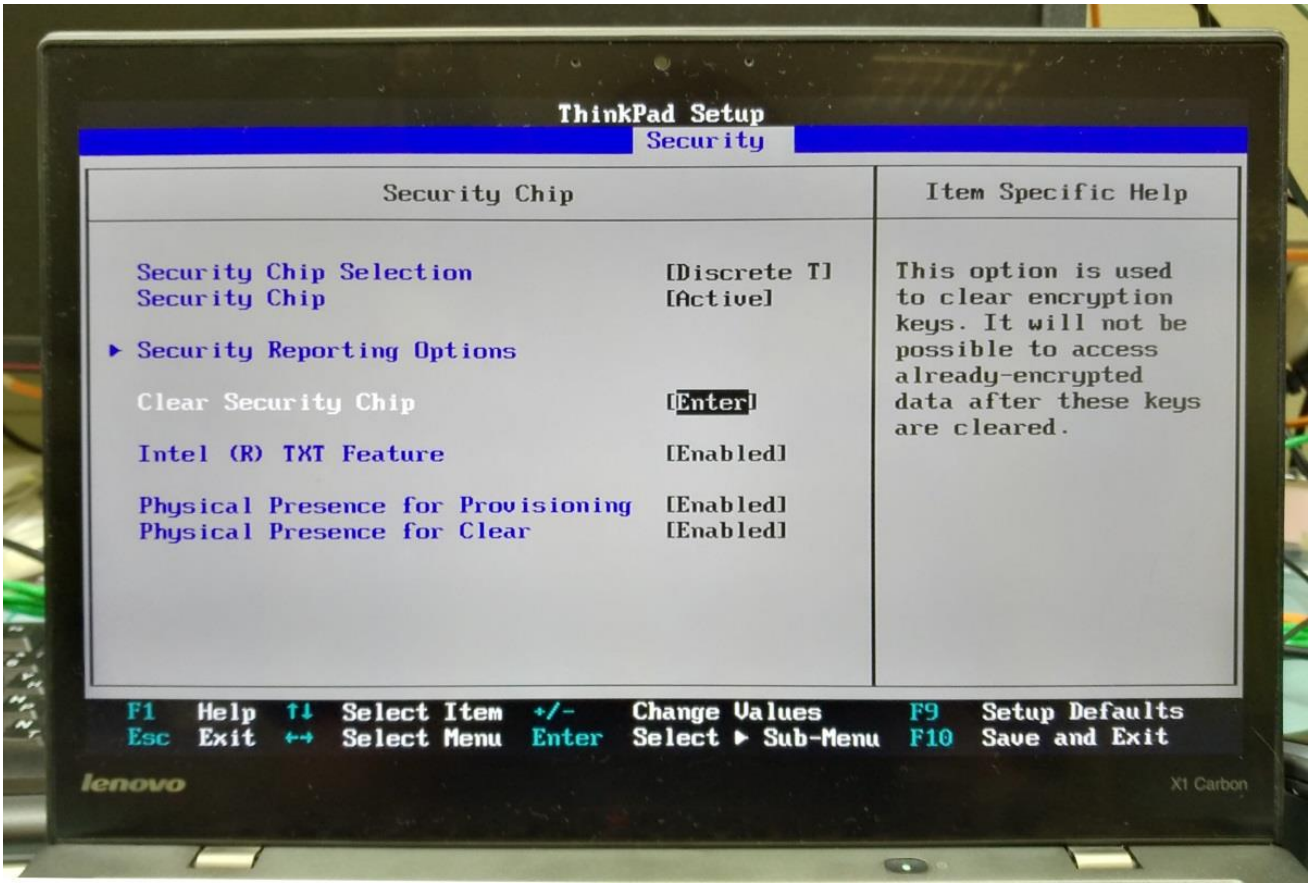


Рис. 4.7 - Очищення пам'яті чипа TPM

Очищення TPM може стати в нагоді, якщо ви, наприклад, захочете продати свій комп'ютер. Врахуйте, що стерши ключі, ви не зможете відновити дані, закодовані цими ключами (якщо, звичайно, ви шифруєте свій жорсткий диск).

Тепер збережіть зміни ("Save and Exit" або клавіша F10), щоб перезапустити комп'ютер.

Після завантаження комп'ютера відкрийте диспетчер пристроїв і переконайтеся, що довірений модуль з'явився в списку пристроїв. Він повинен знаходитися в розділі «Пристрої безпеки», як показано на рис. 4.8.

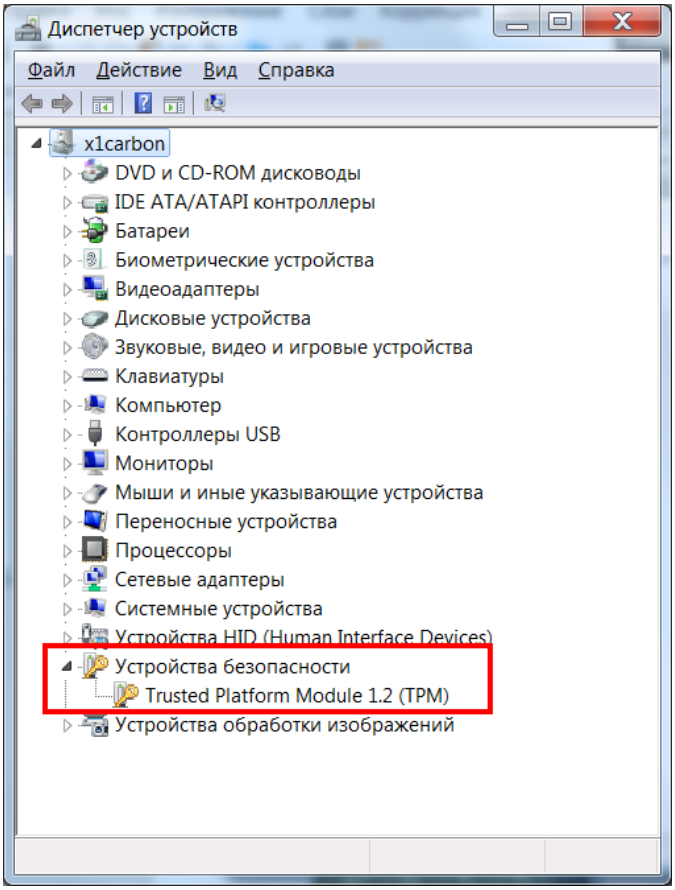


Рис. 4.8 - Чіп TPM в диспетчері пристроїв Windows

4.10. Ініціалізація модуля TPM в Windows

Залишилося форматувати чіп в операційній системі. Для цього потрібно відкрити оснастку управління модулем TPM. Натисніть кнопки Windows + R (відкриється вікно «Виконати»), введіть у поле введення tpm.msc і натисніть «Введення». Запуститься оснащення «Управління довіреною платформним модулем (TPM) на локальному комп'ютері» (див. рис. 4.9).

У правій частині оснащення знаходиться меню дій. Натисніть «Ініціалізувати TPM ...». Якщо ця можливість не активна, значить, ваш чіп вже ініціалізован. Якщо він ініціалізован не вами, а ви не знаєте пароль власника, то бажано виконати скидання і очищення пам'яті модуля, як описано в попередньому пункті.

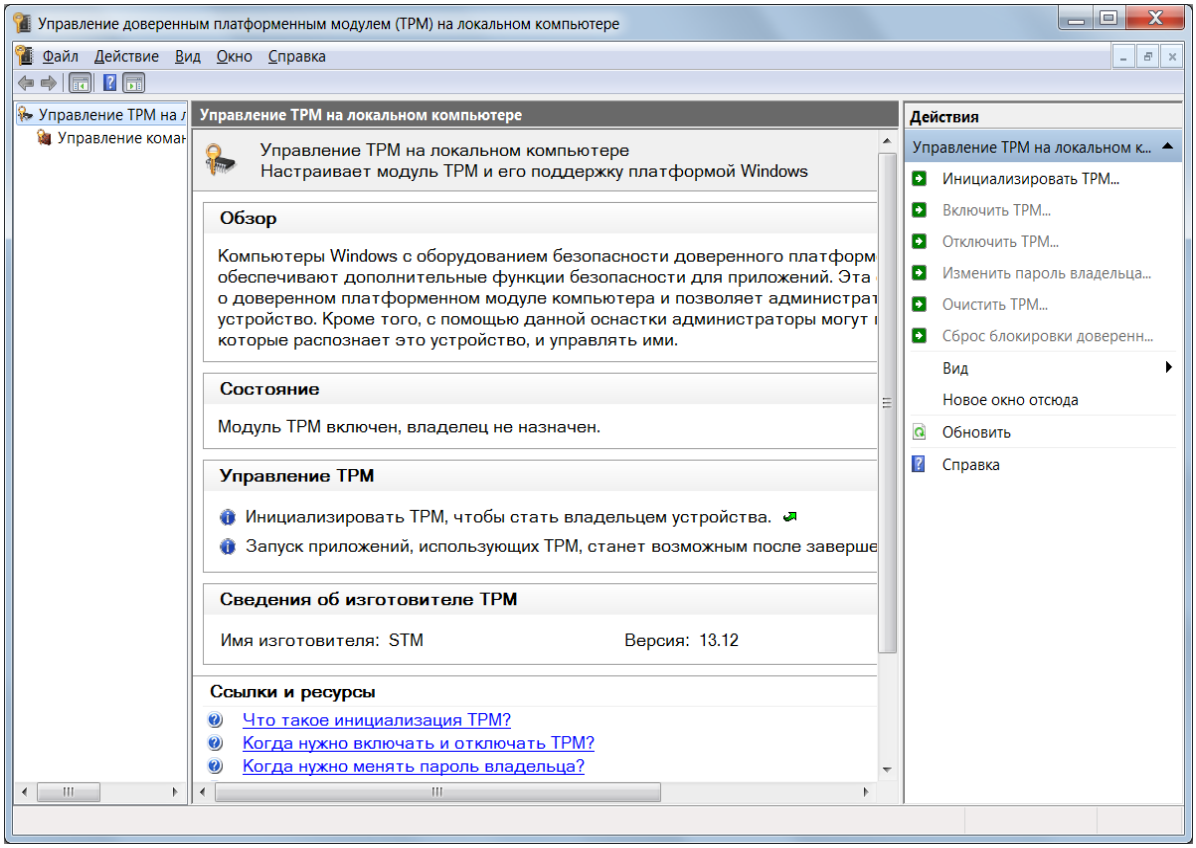


Рис. 4.9 - Оснащення для управління чипом TPM

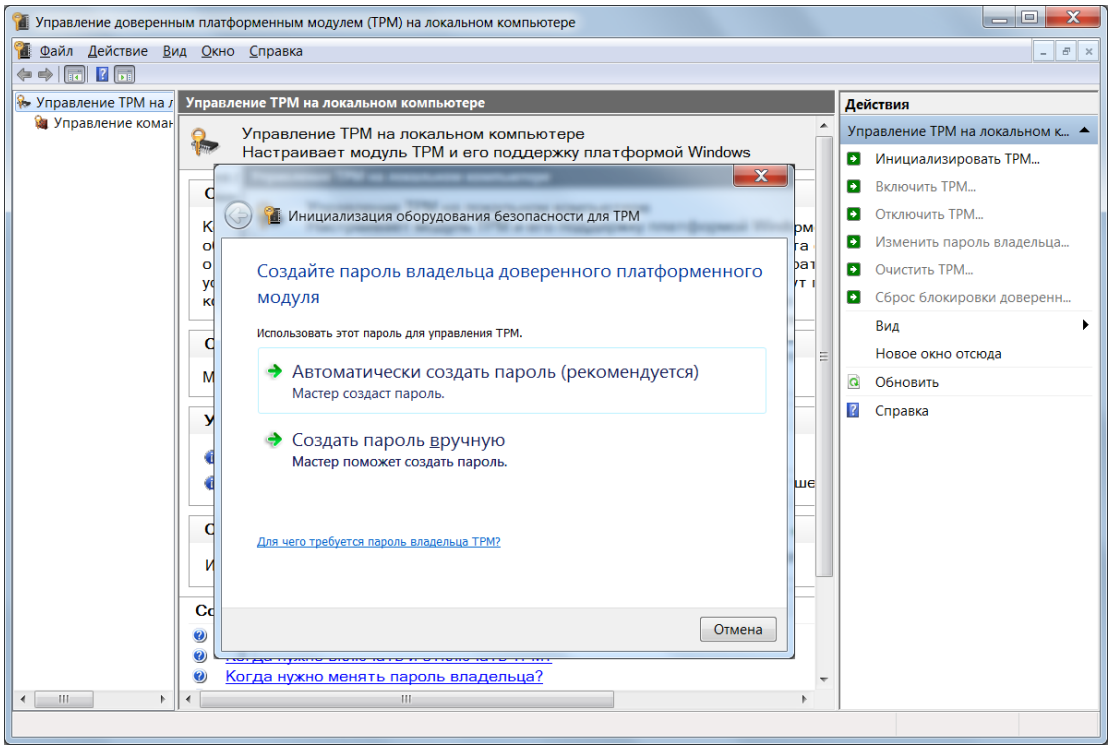


Рис. 4.10 - Пароль власника для TPM створений

Коли запуститься майстер ініціалізації TPM, він запропонує створити пароль. Виберіть варіант «Автоматично створити пароль» (див. рис. 4.10).

По завершенні програма повідомить про успішну ініціалізації модуля (див. рис. 4.11). Після завершення ініціалізації всі подальші дії з модулем - відключення, очищення, відновлення даних при збої, відновлення роботи - будуть можливі тільки за допомогою пароля, який ви тільки що отримали.

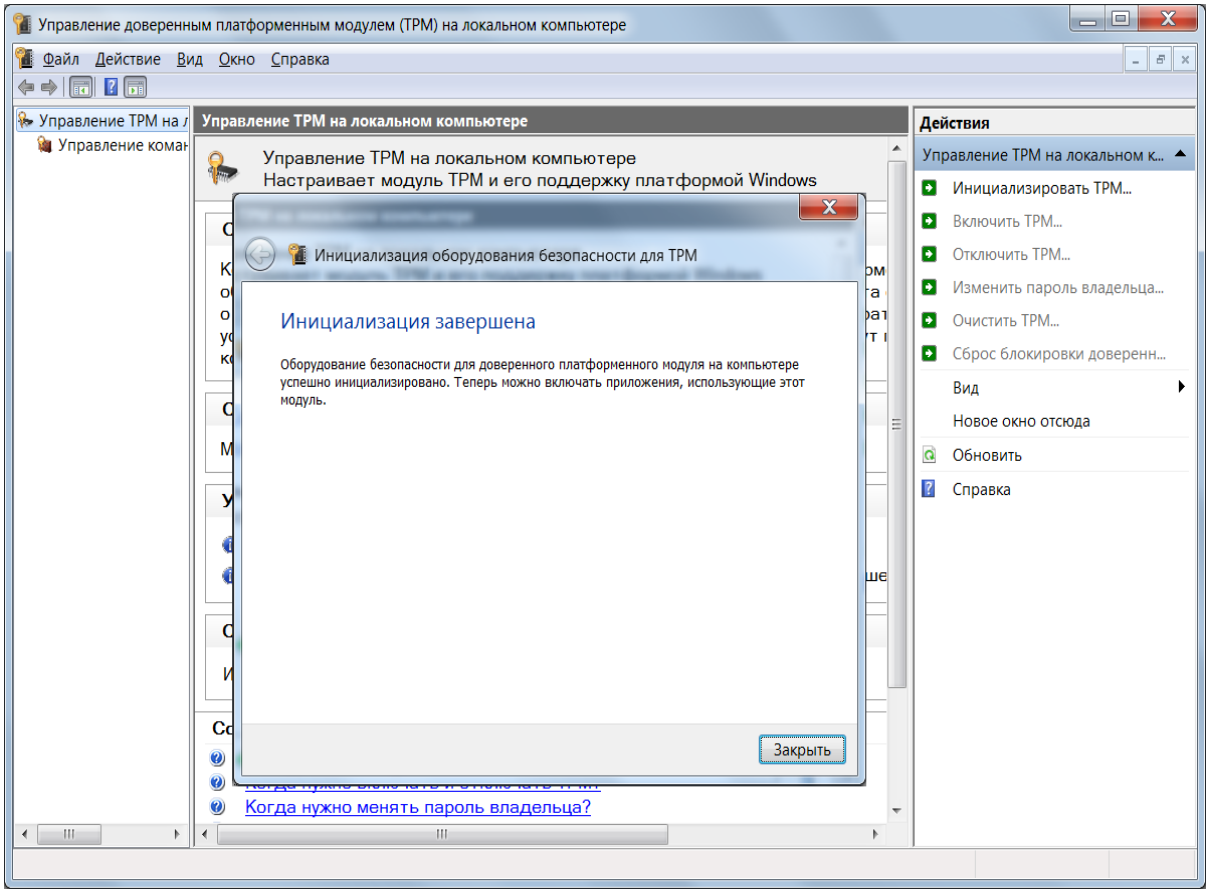


Рис. 4.11 - Ініціалізація TPM завершена

Тепер дія ініціалізації стала неактивною, зате з'явилася можливість відключити TPM, змінити пароль власника і скинути блокування модуля, якщо це сталося (модуль блокує сам себе для запобігання шахрайства або атаки).

Всі подальші операції з чіпом будуть відбуватися автоматично - прозоро для операційної системи і непомітно для вас. **[10]**

ВИСНОВОК ДО РОЗДІЛУ 4.

В цьому розділі було детально досліджено роботу TPM модулю який є невід'ємною частиною Intel TXT.

Було розроблено детальну інструкцію для налагодження цього модулю, а також описано створення основних сутностей і використання основних функцій.

Отриманий досвід та скріншоти були використані для створення урока з учбового курсу на Moodle для вивчення можливостей технології Intel TXT.

ВИСНОВКИ

Метою дипломного проекту було дослідження можливостей технології Intel vPro: Trusted Execution-Technology та розробка програмних засобів навчання використанню можливостей цієї технології у віртуальному навчальному середовищі Moodle.

Для досягнення цієї мети мною була розглянута платформа Intel vPro та основні механізми однієї з її найголовніших технологій - Intel TXT. Були визначені основні функції, методи встановлення довіри, та основні компоненти TXT. Intel TXT стає все доступнішим на все більшій кількості серверних платформ на базі сімейства процесорів Intel Xeon від різних системних постачальників. Постійно зростає екосистема підтримки гіпервізорних та захисних програмних продуктів, яким тепер довіряють, що дозволяє використовувати надійні пули та використовувати моделі відповідності.

Я визначив необхідний функціонал та вимоги до запуску технології. Було реалізовано серверну платформу Moodle, що орієнтована на вивчення персоналізованої навчальної програми по використанню можливостей технологій Intel® vPro™.

Мною було детально досліджено роботу TPM модулю, який є невід'ємною частиною Intel TXT та розроблено інструкцію для налагодження цього модулю, а також описано створення основних сутностей і використання основних функцій. Отриманий досвід та скріншоти були використані для створення урока з учбового курсу на Moodle для вивчення можливостей технології Intel TXT.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Технология Intel® vPro [Електронний ресурс] // team.ru – Режим доступу до ресурсу: http://www.team.ru/lab/intel_vpro.shtml.
2. Организация дистанционного обучения в Moodle [Електронний ресурс] // Osvita.ua. – 2020. – Режим доступу до ресурсу: https://ru.osvita.ua/vnz/high_school/72285/.
3. Как установить Moodle: пошаговая инструкция [Електронний ресурс] // iSpring. – 2018. – Режим доступу до ресурсу: https://www.ispring.ru/elearning-insights/moodle/install.
4. Intel® Trusted Execution Technology: White Paper [Електронний ресурс] // Intel.ru. – 2012. – Режим доступу до ресурсу: https://www.intel.ru/content/www/ru/ru/architecture-and-technology/trusted-execution-technology/trusted-execution-technology-security-paper.html.
5. Intel® Trusted Execution Technology (Intel® TXT) Software Development Guide [Електронний ресурс] // Intel.ru. – 2019. – Режим доступу до ресурсу: https://www.intel.com/content/www/us/en/software-developers/intel-txt-software-development-guide.html.
6. William F. Introduction to Trust and Intel® Trusted Execution Technology / F. William, G. James. – Berkeley, CA: University of California, Berkeley, [Книга] 2013. – 133 с. – (Springer Link).Режим доступу до ресурсу: https://link.springer.com/chapter/10.1007/978-1-4302-6149-0_1.

7. Обзор технологии доверенного платформенного модуля [Електронний ресурс] // Microsoft. – 2016. – Режим доступу до ресурсу:https://docs.microsoft.com/ru-ru/previous-versions/mt431893(v=vs.85)?redirectedfrom=MSDN.

8. Информационная безопасность: Trusted Platform Module и Red Pill. Часть 2 [Електронний ресурс] // vmgu.ru. – 2010. – Режим доступу до ресурсу: https://www.vmgu.ru/articles/tpm-virtualization-security.

9. BitLocker [Електронний ресурс] // Microsoft. – 2018. – Режим доступу до ресурсу:https://docs.microsoft.com/ru-ru/windows/security/information-protection/bitlocker/bitlocker-overview.

10. Что такое TPM и как его использовать в Windows [Електронний ресурс] // soltau.ru. – 2018. – Режим доступу до ресурсу: https://soltau.ru/index.php/themes/kompyutery-iprogrammy/item/501-chto-takoe-tpm-i-kak-ego-ispolzovat-v-windows.

ДОДАТОК 1

«Програмні засоби навчання системних адміністраторів використанню можливостей технологій Intel®vPro™: Trusted Execution-Technology»

Функціональна схема

АРКУШІВ 1

Київ – 2020

ДОДАТОК 2

«Програмні засоби навчання системних адміністраторів використанню можливостей технологій Intel®vPro™: Trusted Execution-Technology»

Принципова схема алгоритму

АРКУШІВ 1

Київ – 2020

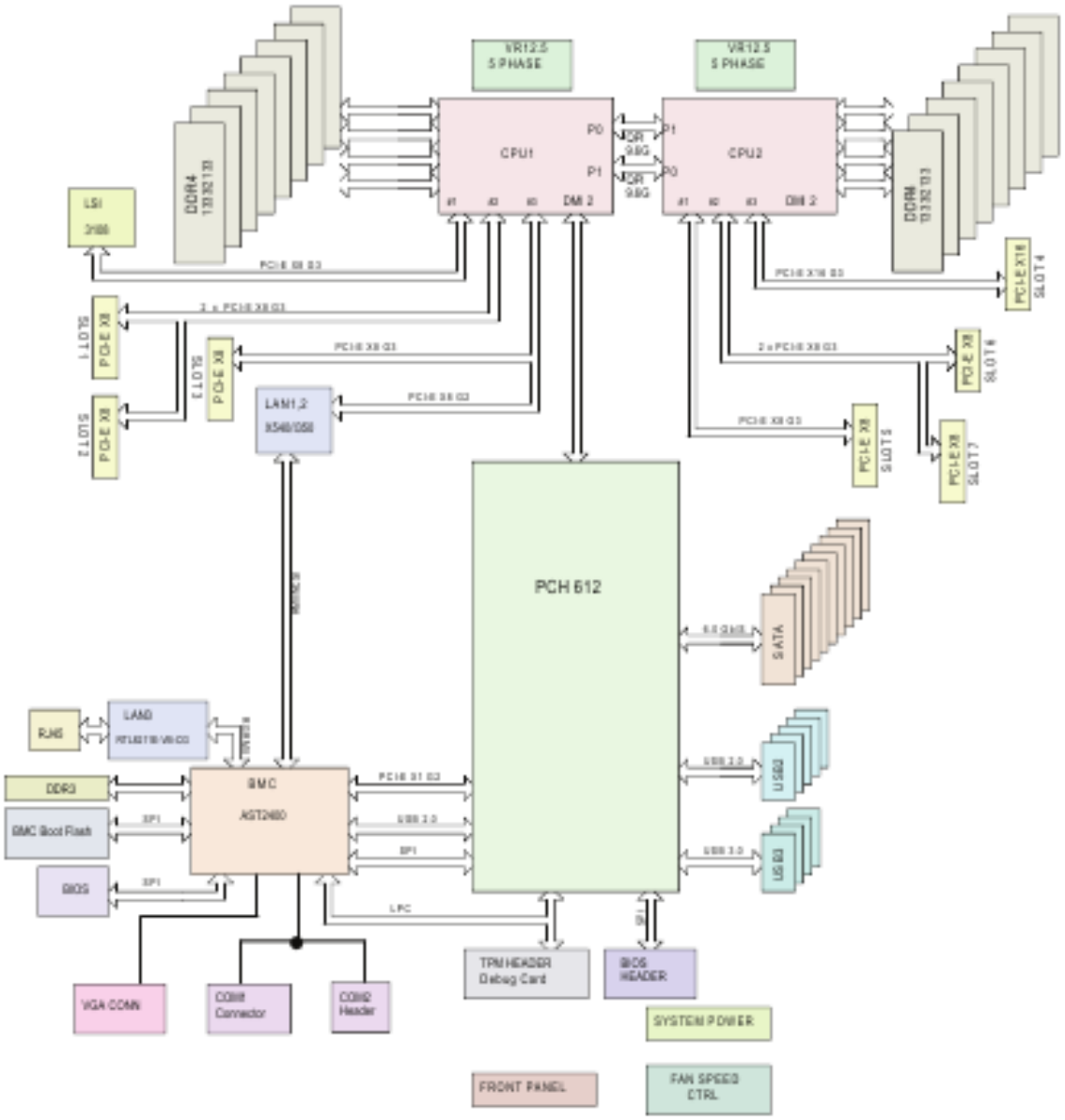
ДОДАТОК З

«Програмні засоби навчання системних адміністраторів використанню можливостей технологій Intel®vPro™: Trusted Execution-Technology»

Структурна схема

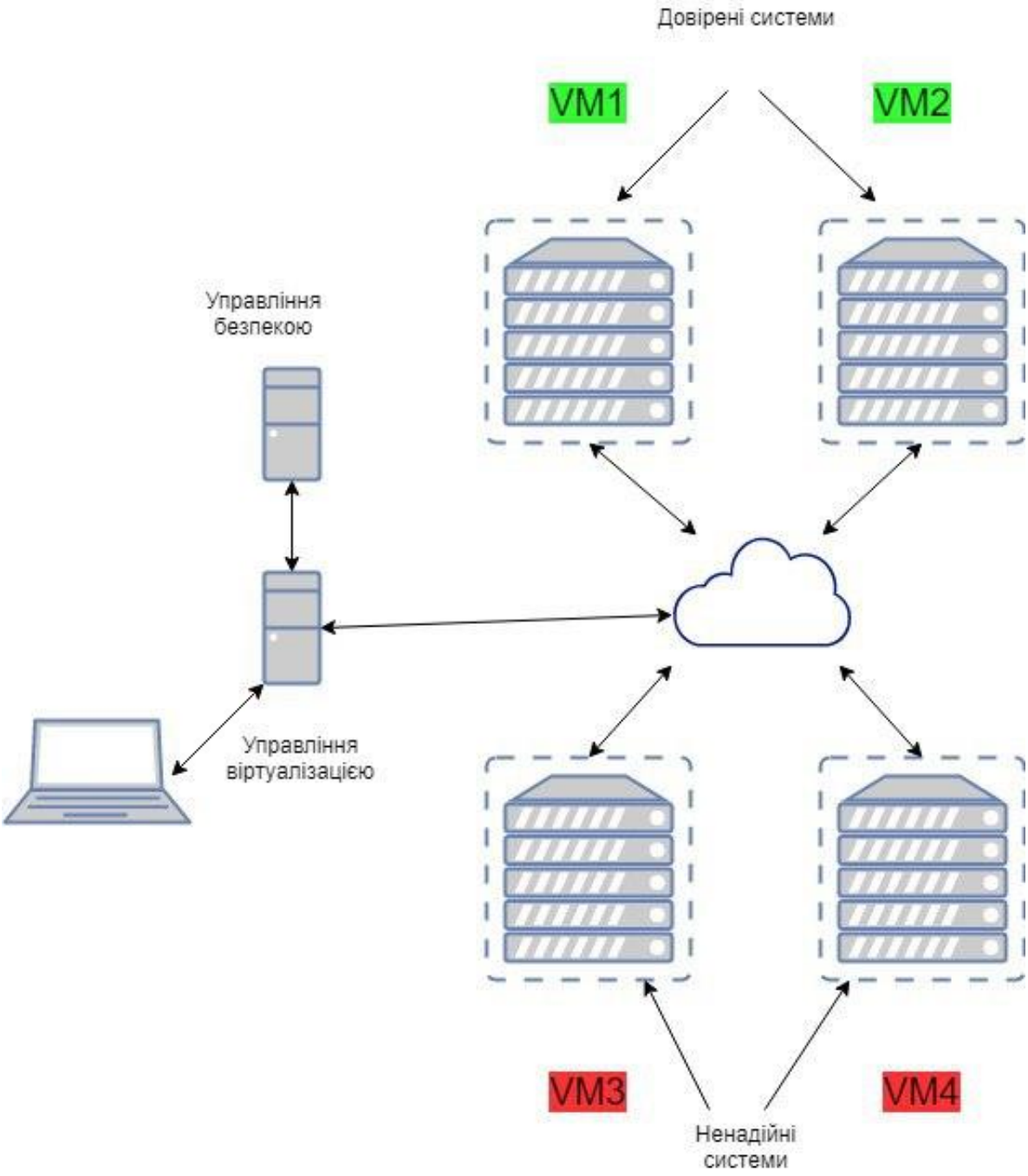
АРКУШІВ 1

Київ – 2020



					ІАЛЦ.467200.004 Д1		
Изм.	*Лист*	*№ докум*	*Подпись*	*Дата*			
Разраб		*Балаценко Г.І.*			Функціональна схема	*Литера*	*Лист*	*Листов*
Пров		*Долголенко О.М.*				*у*	*1*	*1*
						НТУУ «КПІ» ФІОТ ІО-61		
Н. Контр.		*Симоненко В.П*						
Утв								

					ІАЛЦ.467200.004 Д2	
Изм.	*Лист*	*№ докум*	*Подпись*	*Дата*		
Разраб		*Балаценко Г.І.*			Принципова схема алгоритму	*Литера* / *Лист* / *Листов*: *у* / 1 / 1
Пров		*Долголенко О.М.*				
Н. Контр.		*Симоненко В.П*				***НТУУ «КПІ» ФІОТ ІО-61***
Утв						



					ІАЛЦ.467200.004 ДЗ	
Изм.	*Лист*	*№ докум*	*Подпись*	*Дата*		
Разраб		*Балаценко Г.І.*			Структурна схема	*Литера* / *Лист* / *Листов*: *у* / *1* / *1*
Пров		*Долголенко О.М.*				
Н. Контр.		*Симоненко В.П*				***НТУУ «КПІ» ФІОТ***
Утв						***ІО-61***